IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff	)	
	)	
-VS-	)	Criminal No. 21-10104-PBS
	)	Pages 2-1 - 2-153
VLADISLAV KLYUSHIN,	)	
	)	
Defendant	)	

JURY TRIAL - DAY TWO

BEFORE THE HONORABLE PATTI B. SARIS
UNITED STATES DISTRICT JUDGE

United States District Court
1 Courthouse Way, Courtroom 19
Boston, Massachusetts 02210
January 31, 2023, 8:46 a.m.

LEE A. MARZILLI
KATHLEEN SILVA
OFFICIAL COURT REPORTERS
United States District Court
1 Courthouse Way, Room 7200
Boston, MA 02210
leemarz@aol.com

APPEARANCES:

SETH B. KOSTO, ESQ. and STEPHEN E. FRANK, ESQ., Assistant United States Attorneys, Office of the United States Attorney, 1 Courthouse Way, Room 9200, Boston, Massachusetts, 02210, for the Plaintiff.

MAKSIM NEMTSEV, ESQ., 20 Park Plaza, Suite 1000, Boston, Massachusetts, 02116, for the Defendant.

MARC FERNICH, ESQ., Law Office of Marc Fernich, 800 Third Avenue, Suite Floor 20, New York, New York, 10022, for the Defendant.

INDEX

P R O C E E D I N G S

THE COURT: Good morning.

MR. FRANK: Good morning, your Honor.

MR. NEMTSEV: Good morning, Judge.

THE COURT: We're only up to nine jurors, so hopefully they'll make it through the frigid weather. Did you need to see me on anything?

MR. NEMTSEV: I did, your Honor. I wanted to see you about -- there's no dispute amongst the exhibits, what's coming 08:46 in and what we can -- there's a small dispute. It's small. It's actually very small. There's one exhibit. It's log files totaling a million and a half, or whatever it is. It's a huge exhibit. It's a spreadsheet. In that exhibit there's various columns, and I believe those were pulled from one of the filing agent servers. In those columns, the filing agent or their log files say this IP is associated with Delaware, or this IP is associated with the Republic of Korea.

Now, the government says I'm not entitled to use that because I contested MaxMind's analysis, but I think it's part 08:47 of the record that's in evidence.

THE COURT: Well, if it's in evidence -- is it in evidence?

MR. KOSTO: Your Honor, that exhibit is in evidence, but they would be seeking to have their cake and eat it too. They moved to exclude MaxMind as unreliable. That column of the exhibit comes from MaxMind and similar databases. So to suggest --

THE COURT: I know, but if it's in evidence, can't he point to it? You've put it in evidence.

MR. FRANK: But, your Honor, we are redacting things all the time at their request. Here what they're asking for is the exact stuff that they don't want us to rely on. So it's fine. If that's what they want to point to, then we get the MaxMind data.

08:47 THE COURT: Do you know where it's from?

MR. NEMTSEV: No, I don't. From what the government told me, it's from Microsoft.

THE COURT: Let me put it this way: If it's an exhibit, you can point to it, but that might open the door.

MR. KOSTO: But if Microsoft --

THE COURT: Excuse me. If it's in the "in," it's a marked exhibit, they can point to it. But then you will have to ask what's that based on, and if the answer is MaxMind, which it sounds as if it is --

08:48 MR. FRANK: The answer will be Microsoft. Then we have to go down the rabbit hole of Microsoft collects it from places like MaxMind.

THE COURT: It is what it -- what can I do if it's in evidence? Have you redacted it?

MR. FRANK: Well, this just came up 20 seconds ago, so --

THE COURT: But you knew it was in evidence. It says Delaware. I'm just saying, what's sauce for the goose is sauce for the gander.

MR. FRANK: And that's exactly our point, Judge, if he wants to put it in, but we can't --

THE COURT: He's not putting it in. You're putting it in, right?

MR. FRANK: But he's relying on --

08:48 THE COURT: Excuse me. If it's in evidence, he can ask about it. It may open the door.

MR. FRANK: Well, then we'll redact it, but we don't have -- like, then we'll need some time to redact that particular --

THE COURT: We could just mark it for identification, but, understand, it might open the door. What do you want to do?

MR. NEMTSEV: Can I have two minutes to think about that?

08:49 THE COURT: Yes. I mean, you don't have to -- when is it coming?

MR. NEMTSEV: This would be the third witness, I believe? Not the first, the third.

THE COURT: Because it could just be that he's willing to allow it in about MaxMind but point out how confusing it is and it's all over the place. But you're going to have to make a decision because what's sauce for the goose -- isn't that the expression? -- is sauce for the gander. It may not translate well into Russian. However, you get the point.

MR. NEMTSEV: I do get the point.

THE COURT: Okay, all right. What number was this that we've been talking about?

MR. NEMTSEV: This is Exhibit 71, your Honor.

MR. KOSTO: And practically speaking, your Honor,
08:49 Exhibit 71 is a thumb drive with millions of lines of code in it that would be all but impossible to redact.

THE COURT: Well, I understand that, but --

MR. KOSTO: What we would propose is that the parties not examine on that particular issue within the logs. The jury won't be able to access it and see it.

THE COURT: Well, that's overruled. If it's in, it's in. But what I'll do is, I'll mark it for identification. I'll let them make a decision. What do you want to do?

MR. FERNICH: Let me and Max --

08:50 THE COURT: Why don't you talk, talk amongst yourselves, and then I will -- but I'll let them point out the other, okay? If it says Boston through MaxMind -- isn't that the name of it?

MR. KOSTO: Yes, your Honor.

THE COURT: -- I'll just perhaps -- maybe, if you don't ask about it, I won't let them ask about it. Meanwhile, I'll mark it for identification when it comes in, and it may be subject to redaction. I have no idea what it is. I've heard about this for the first time this morning.

MR. NEMTSEV: I think it's going to be impossible, your Honor, not to ask about it because the witnesses, the ones that did the investigation, they use this stuff to --

THE COURT: Then I'll let them ask, okay?

MR. NEMTSEV: Thank you, Judge.

08:51 THE COURT: Okay. That's it. Good. We're waiting for the other nine jurors.

MR. FRANK: So that means that the MaxMind data comes in if they ask about it?

THE COURT: If they ask about it, you can ask about it.

MR. FRANK: Well, we would be asking about the MaxMind data, but that's a different witness.

THE COURT: Maybe it is. I don't know. I can't --

MR. FERNICH: It's hard to rule on this in a vacuum

08:51 because I don't know what he's going to ask about it. It could be a one-question thing and gone, goodbye. I mean, we really don't know what it is.

THE COURT: It depends what the answers are. I will listen and I will be instructed, but I can't let you do one thing that I don't allow them to do.

MR. NEMTSEV: I understand.

MR. FRANK: Thank you, Judge.

THE COURT: Do you need me? Perfect.

(Discussion off the record.)

(A recess was taken, 8:58 a.m.)

(Resumed, 9:20 a.m.)

THE COURT: You're still under oath, the interpreters. Thank you.

THE CLERK: Okay, let me get the jury. It's going to
09:20 take a second, Judge.

THE COURT: The last juror just arrived.

MR. KOSTO: Your Honor, would you like Mr. Brawner on the stand now?

THE COURT: That's a great idea.

THE CLERK: All rise for the jury.

(Jury enters the courtroom.)

THE COURT: Thank you. Good morning. You may be seated. Let me ask you, did anyone speak about this case? Did anyone see anything in the press? Anyone see anything in
09:22 social media? Anyone communicate with any of you? All right, I find the jury has complied.

And I do understand we're getting going a little late because one or two of you were delayed. Of course, as Murphy's law would have it, we had a little snow this morning, but whoever was late -- I forget -- did the right thing and called

Jury. But right now we have two new numbers for you to call because the jury staff isn't always in when a jury isn't being impaneled. So we've given you the numbers that you can call, Maryellen or Maya, if there's a delay, so that way we know, as we did this morning, which was great, exactly what's happening.

The second thing is, if for some reason you get lost, just don't walk into this room. You never know what issue we may be arguing; for example, maybe something you shouldn't hear. So if there's an issue, just go back down to the second 09:23 floor and ask them for help in getting upstairs.

So right now we're starting with I believe our first witness. You all have your notebooks, pens? And hopefully your tech is still working, although we're always crossing our fingers.

So go ahead, Mr. Kosto.

MR. KOSTO: The United States calls Marcus Brawner.

THE CLERK: Sir, could you please stand and raise your right hand.

MARCUS BRAWNER

09:23 having been first duly sworn, was examined and testified as follows:

THE CLERK: Could you please state and spell your last name.

THE WITNESS: My last name is Brawner, B-r-a --

THE COURT: Uh-uh. We can't hear you. This is a giant-sized room. So pull in this mic here so we can really hear.

THE WITNESS: All right. Brawner, B-r-a-w-n-e-r.

THE CLERK: Thank you.

MR. KOSTO: May I proceed, your Honor?

THE COURT: Yes.

DIRECT EXAMINATION BY MR. KOSTO:

Q. Mr. Brawner, would you pull that microphone nice and
close. We'll let you know if it's too loud, and I'll do my
09:24 best to --

THE COURT: It's always a fine art because sometimes it's so close, it pops Lee's ears. So we just want to make sure, though, that the jury can hear.

And if you can't hear, just raise your hand and say "I can't hear." All right.

MR. KOSTO: Your Honor, the government would offer Exhibits 237, 238, 239 and 240, 73, 74 --

THE COURT: Wait, wait, wait, wait. We don't speed read here.

09:24 MR. KOSTO: I'll slow it down.

THE COURT: 237, 238 --

MR. KOSTO: 238, 239, 240, 73, 74, 75, and 77-A for identification.

THE COURT: All right.

MR. NEMTSEV: No objections, your Honor.

(Exhibits 237-240, 73-75 received in evidence.)

(Exhibit 77A marked for identification.)

BY MR. KOSTO:

Q. Good morning, Mr. Brawner.

A. Good morning.

Q. What city do you work in, sir?

A. Nashville.

Q. And where do you work?

A. I work for a company called Kroll.

09:25 Q. What is Kroll's business?

A. Kroll is in the business of providing risk advisory, investigation, and response services.

Q. Do you work with any particular division of Kroll?

A. I work in the Cyber Risk Division.

Q. And what's the Cyber Risk Division?

A. Cyber Risk provides a range of cyber security services for clients, both preventive in terms of helping them prepare for security, as well as responding and investigating into incidents or intrusions and the like.

09:26 Q. You mentioned incidents. Can you describe the term "incident response" for the jury.

A. Sure. Incident response is the discipline of investigating and responding to and containing a cyber intrusion. So, in other words, if someone has broken into a system, our job is to help identify that and get that person or that issue resolved.

Q. What is your title at Kroll, Mr. Brawner?

A. Managing Director.

Q. And how long have you worked in the incident response field?

A. Over twenty years.

Q. Are you familiar with the company Toppan Merrill?

A. Yes.

Q. Is it sometimes referred to as TM?

09:26 A. Yes.

Q. And where is that company headquartered?

A. I believe Toppan is headquartered in Minnesota.

Q. Let me ask you, in late 2019 and early 2020, did Kroll Cyber Risk get involved to investigate a possible intrusion on Toppan Merrill's computer network?

A. We did.

Q. And what was your role in that response?

A. I was one of the lead investigators on that response.

Q. From your involvement, do you know what Toppan Merrill's
09:27 business is?

A. My understanding is, Toppan Merrill provides business services in the area of printing and financial applications to help companies prepare things like government filings for their businesses.

Q. And are you familiar with how often those filings that you described takes place in Toppan Merrill's business?

A. My understanding and from what I saw was, quarterly or annually is typical.

Q. Are companies like Toppan Merrill sometimes called "filing agents"?

A. Yes.

Q. What were the names of the Toppan Merrill computer systems that you were responding to in this incident response?

A. We looked at two primary --

09:28 THE COURT: Now, when you say "we" --

THE WITNESS: Kroll.

THE COURT: Did you personally?

THE WITNESS: Yes, myself and our team. I looked at two systems in particular. One was an application called Bridge and one was an application called UIT.

Q. Let's start with UIT. Do you know what that stands for?

A. It stands for Unit Investment Trust.

Q. And in general terms, what was the Unit Investment Trust system at Toppan Merrill?

09:28 A. It was an Internet-facing Web application used by some of its financial clients.

Q. The other system you mentioned was the Bridge system, correct?

A. Yes.

Q. And what was the Bridge system?

A. The Bridge was another Internet-facing application, as well as a desktop computer application, used by its clients in the preparation of filings for the SEC and so forth.

Q. And where was the Bridge system physically located, the computers themselves?

A. The Bridge system included systems in Minnesota as well as in the cloud, in the Microsoft cloud.

Q. And was each of them, Bridge and UIT, accessed by way of the Internet?

09:29 A. Yes.

Q. Let's start with a few terms that might be helpful for the jury. Can you tell the jury what an Internet domain is.

A. Sure. An Internet domain is the name -- what we think of as the name of a website that we visit. So if you visit Google.com, Google.com is an Internet domain.

Q. How about an IP address or Internet protocol address?

A. So an IP address is a series of four numbers separated by dots, so it would be something like 123.45.67.89. And an IP address is much like a phone number that we would think of; it represents a system on the Internet. 09:30

Q. So if I went to your domain example, Google.com, is there an IP address that goes with Google.com?

A. Yes.

Q. And if I went to an IP address associated with Google.com on my browser, would I end up at Google.com?

A. Yes. So when you enter Google.com, your computer will make a query to what's called a "domain name server," and that server will tell your computer the IP address to use to connect to Google.com at that point.

Q. It's fair to say the domain name server you described is kind of like a phonebook?

A. Much like a phonebook, an address book.

THE COURT: What exactly is a server?

THE WITNESS: So a server would be a computer that is
09:31 used to provide services to people or other systems. So a desktop computer --

THE COURT: It's a piece of machinery?

THE WITNESS: It is a piece of machinery, yes.

Q. And in the context of the Judge's question about server, what is a client?

A. So we would refer to a client -- I would refer to a client as the end user of a system. It could also refer to the software that you as a person might interact with on your laptop or your desktop computer.

09:31 Q. In late 2018, what was the domain for the UIT system?

A. There were two domains for UIT in late 2018. One was UIT.MerrillCorp.com and the other was UIT.ToppanMerrill.com.

Q. As part of the incident response, did you examine records of activity on the UIT system?

A. Yes.

Q. Can you explain to the jury what logs are.

A. Logs are, in effect, an audit trail of activity on a computer or related to an application. So logs, if you receive a phone bill at home, it shows an accounting of all the calls that you made in a given month; that would be an example of a log.

Q. But in this case for the computer's activities, not the phone?

A. Correct, in this case, for a specific system.

09:32 Q. When was the first suspicious access that you identified to the Toppan Merrill UIT network?

A. Our investigation found an initial compromise and breach of that system in late November of 2018.

Q. Let me ask you, Mr. Brawner, to look at Exhibit 237, which is in evidence and should be up on the screen in front of you. Do you have it there?

A. Yes.

MR. KOSTO: Your Honor, do you have it?

THE COURT: Is it coming up on all your computers?
09:33 Now, you can touch the computer screen, so if you --

THE CLERK: It's not working.

THE COURT: He can't underscore?

THE CLERK: No. It's broken, unfortunately.

MR. KOSTO: I just lost it on my screen, your Honor. I'll use this one. Oops, it's back.

Q. What is Exhibit 237, Mr. Brawner?

A. This is a web server log from UIT. So this is a log showing activity that was taking place on the UIT web server on November 28, 2018.

Q. And has Ms. Lewis highlighted the date that you've just read aloud?

A. Yes.

Q. And approximately what time do these log entries on Page 1 of Exhibit 237 refer to?

09:34 A. They show 11:41:01.

Q. And looking at Pages 1 -- and I'll ask Ms. Lewis to take you forward to Page 2 and Page 3 -- and, Ms. Lewis, if you could take us back to Page 1 -- what activity is Exhibit 237 showing on the UIT system?

A. Each row or each section of the log represents one request from a client computer to the UIT server requesting for a specific file name.

Q. Is there a piece of software that is running in these logs?

09:35 A. Yes.

Q. What is the name of the software that's running? And if it's reflected, could you point us to where it is.

A. So at the end of the second row of each log entry is a reference to a program named DirBuster, D-i-r-b-u-s-t-e-r, the OS/2 DirBuster project.

Q. What is DirBuster?

MR. NEMTSEV: Objection, your Honor.

THE COURT: Overruled. If you know.

A. DirBuster is a freely available tool that can be used to perform what we call brute force attacks against a server; in other words, to try to guess and identify valid file names or valid paths on a server.

Q. You said "brute force." What is that?

A. So brute force means the idea of rapidly and thoroughly 09:35 guessing or attempting to guess valid information. We often think about our personal passwords being compromised by a brute force attack; someone guessed my password by trying all possible words in a dictionary, for instance.

Q. So if I had a four-digit password, what would be a brute force attack on that password?

A. So I would try 0000 through 9999.

Q. And how do you recognize this DirBuster code in Exhibit 237 as a brute force attack?

A. In this case, we see multiple requests during the same 09:36 second, so each entry that's shown occurred at 11:41:01 seconds.

Q. Is that true of every entry on Pages 1, 2, and 3?

A. Yes.

Q. Was DirBuster an authorized program on Toppan Merrill's network?

A. No.

Q. Let me show you Exhibit 238. It's just one page. First of all, do you recognize it?

A. Yes.

Q. And what is it?

A. This is a view of a Microsoft Windows security log dated December 25, 2019.

Q. Christmas Day?

A. Christmas Day.

09:37 Q. And does the log that you're talking about here show what computer it's from?

A. Yes.

Q. Where is that?

A. In the lower right, the last line indicates the computer from which this event was recorded.

Q. Would you read the name of the computer, please.

A. It's USD10846.TM.ToppanMerrill.com.

Q. Do you know what "USD" stands for on Toppan Merrill's network?

09:38 A. Yes.

Q. What is that?

A. It signifies a U.S., United States, desktop computer, the "D" meaning desktop.

Q. And in Toppan Merrill's naming system, what typically follows USD for desk tops?

A. A string of digits much like a serial number or an asset number.

Q. Numbers or letters?

A. Numbers.

Q. What about USL?

A. So the "L" in USL would represent a laptop, so a U.S., United States, laptop computer.

Q. Did you also see computers named with the first two letters "NA"?

09:38 A. Yes.

Q. And what did that correspond to in Toppan Merrill's naming convention?

A. North America.

Q. What time is the log in Exhibit 238?

A. 4:48:54 a.m.

Q. And do you know what times on that is?

A. That was U.S. Central Time.

Q. Early in the morning?

A. Before business hours, yes.

09:39 Q. And if I can direct you to the middle of the log, there's a row that reads "New Process Name." Do you see that there?

A. Yes.

Q. What is the log showing when it says "New Process Name"?

A. So this log indicates that an application named migrate.exe was started. So think about if you launch your Web browser, you're launching a new process.

Q. And did you look at --

THE COURT: I don't understand what you just said.

Q. What's a process?

A. So a process is --

THE COURT: Don't forget, you're talking, just assume me, okay? Not a sixteen-year-old. So just bring it so that everyone here can understand it, all right?

THE WITNESS: Sure. So any program that you're
09:40 running on your computer runs as a process. So a process is an instance of some software that is running on your computer. So your web browser, Microsoft Word, your e-mail software, each would be running as one or more processes on the computer.

THE COURT: All right, so what did we just look at?

Q. So if your example is processes like Microsoft Word or Safari, the browser, or Outlook, the e-mail program, what is the program that's showing up in this log as running?

A. So this log is showing a program named migrate.exe running.

09:40 Q. Did you look at what migrate.exe was on Toppan Merrill's system?

A. We did.

Q. And what was it?

A. It was a renamed copy of a program called PuTTY or PLINK.

Q. And in the plainest of English, what is PuTTY or PLINK as a program?

A. PuTTY or PLINK is a tool often used by system administrators to connect to a remote computer for purposes of managing that. So it allows you to create a secure connection to another computer.

Q. When you say a remote computer, what do you mean?

A. So a computer other than the one that you are physically sitting at or connecting with.

Q. And when you say administrator, are we talking IT 09:41 department?

A. Yes, most often.

Q. Okay. So you mentioned that migrate.exe was a renamed version of PuTTY or PLINK, correct?

A. Yes.

Q. What was the significance to you, as an investigator, of the renaming of PuTTY to a different name?

A. As an investigator, we often --

MR. NEMTSEV: Objection, your Honor.

THE COURT: Overruled.

09:42 A. -- we often see individuals who are trying to hide their tracks or perform unauthorized actions may choose to rename a file to something other than what it is to hide from the view of a security team or someone that might review these logs.

MR. NEMTSEV: Objection, your Honor. I move to strike that. He's not been noticed as an expert, and he's testifying about hypotheticals, "often see, often do."

THE COURT: I'll allow it just in terms of what his state of mind was as he's investigating this, not that that's what happened, unless I hear that later.

A. Additionally, the path on the computer where the program is running from is not a typical path where PuTTY would be installed or PLINK would be installed.

THE COURT: Is PuTTY or PLINK a valid application that's normally used in the course of business?

09:43 THE WITNESS: It can be, yes.

Q. And is a renamed version of PuTTY or PLINK something that Toppan Merrill installed on its network?

A. No.

Q. Let me show you Exhibit 239 in evidence. Do you recognize it?

A. Yes.

Q. Is this another log?

THE COURT: By the way, I want to remind you, I'm asking the questions, but I'm sure some of you have questions. 09:43 If you don't understand a term, raise your hand and ask Maryellen to have it explained, all right? Hand it up to her. Thank you.

MR. KOSTO: May I proceed?

THE COURT: Yes. I'm sorry. Just to make sure everybody is understanding.

Q. What is Exhibit 239?

A. So 239 depicts another Windows event log, in this case, from January 10, 2019.

Q. At what time of day?

A. At 5:42 a.m. Central Time.

Q. Outside of business hours?

A. Outside of business hours.

Q. And what was the machine that this log is for?

A. The computer name this log is for is 09:44 USD10472.adminassist.mrll.com.

Q. Is that the same or a different computer from Exhibit 238? We can go back and look if it's helpful.

MR. KOSTO: Ms. Lewis, would you kindly take us to 238.

Q. What was the computer in 238?

A. It is a different computer. 238 shows USD10846.

Q. And Exhibit 239 shows what?

A. USD10472.

Q. Remind us, USD stands for?

09:44 A. U.S. desktop.

Q. Do you know the user that USD10472 was assigned to?

A. This computer was assigned to a user named Arthur Smallman.

Q. Do you see reference in this document at the line "Source" toward the bottom to the word "PowerShell"?

A. Yes.

Q. Can you explain to the jury what "PowerShell" is. For starters, is it a program?

A. Yes. PowerShell is a component of Microsoft Windows, the operating system that provides typically an administrator of the computer the ability to manage and configure and control that computer. So the word "shell" in technology sense is essentially a command prompt, a place where we can interact with and instruct the computer, and PowerShell is installed on 09:46 virtually all of Microsoft Windows systems.

Q. And in this case, does a user need to be sitting at the computer that they are managing with PowerShell?

A. No.

Q. How does that work if the user of PowerShell isn't sitting at the computer that is being acted on?

A. So PowerShell has the ability to facilitate connections to a remote computer for the purpose of instructing that remote computer. So I can sit at my laptop, for example, and execute commands or instructions on a computer somewhere else over a 09:46 network.

Q. Do you see a reference in the second line of Exhibit 239 to "invoke Mimikatz"?

A. Yes.

Q. What is Mimikatz?

A. Mimikatz is a program that is used to extract or dump passwords from the computer from which it's run, often for, I would say often unauthorized --

MR. NEMTSEV: Objection, your Honor.

THE COURT: Sustained.

MR. NEMTSEV: Move to strike.

Q. What is the date associated with the "invoke Mimikatz" command here?

A. It's January 10, 2019.

Q. And what program was used to initiate that instruction?

09:47 A. PowerShell.

Q. Was Mimikatz, the credential scraping tool, a tool that Toppan Merrill had installed for authorized use on its system?

A. No.

Q. Let me direct your attention to Exhibit 240. It's our last log for now. Do you see it there?

A. Yes.

Q. Do you recognize it?

A. Yes.

Q. What is it?

09:48 A. This is another Microsoft Windows PowerShell log that is depicting the copying of the PowerShell application to another instance with a different name; in other words, creating a copy of PowerShell under a different name, in this case RDTEVC.exe, as shown in the log.

MR. KOSTO: Ms. Lewis, could you please highlight the line that begins "host application."

Q. You mentioned RDTEVC.exe a second ago; is that right?

A. Yes.

Q. What's happening in the line that Ms. Lewis has highlighted? What's the code doing here?

A. So the Windows PowerShell application is being instructed to make a copy of itself into another file named RTDEVC.exe.

Q. So this is a renaming of PowerShell?

A. Effectively, yes.

09:49 Q. And let me take you to the bottom of Exhibit 240, the fifth page, bottom half. Do you have it there?

A. Yes.

Q. Can I ask you, with reference to the last three lines of this code, in human terms, what's going on here?

A. So this is a view of instructions that were passed to PowerShell, in this case asking PowerShell and the computer to make a connection to an internet domain called cloudAPIfinance.info.

Q. Is that in the middle of the first highlighted line?

09:50 A. Yes.

Q. And was establishing a secure connection to cloudAPIfinance.info part of this machine's typical use?

A. No.

Q. Did Kroll and you find other internet domains and IP addresses that Toppan Merrill computers were connecting to during the course of your engagement?

A. Yes.

Q. And can you describe them for the jury generally, these domains.

A. We found several domains that were not known to Toppan Merrill that computers were connecting to. Each of the domains were named in permutations that would suggest that they were finance-related domains. So here it was Cloud API Finance. I believe we also saw FinancecloudAPI.com, and other similar 09:51 domains.

Q. About how many were there?

A. Approximately eight.

Q. And did each of those domains that you found correspond to an IP address?

A. Yes.

Q. And as you sit here today, can you recall the name of each and every one from memory?

A. No.

Q. Did you make a record of them when the names were fresh in 09:51 your mind?

A. Yes.

Q. For identification, I'm showing you Government's Exhibit 77A. Does the unredacted portion of this list accurately describe the domains that you were just testifying to?

A. Yes, it does.

Q. Let me have you read the domains aloud, please.

THE COURT: Well, can we just mark it?

MR. NEMTSEV: Could we just admit it, your Honor?

THE COURT: Yes, I'm with you.

MR. KOSTO: We can admit it, your Honor.

THE CLERK: What number?

MR. KOSTO: 77A.

THE CLERK: It's in.

09:52 MR. KOSTO: And let me ask --

THE COURT: So we already have 77A in. Do you want 77B?

MR. KOSTO: No. I had moved 77A for identification, but we're happy to offer it. We would so offer it. Thank you.

(Exhibit 77A received in evidence.)

Q. Could you read the domains on the two pages of Exhibit 77A.

A. Yes.

THE COURT: You want to sit and read all these?

09:52 MR. KOSTO: There are only eight, your Honor, but, yes.

A. CloudAPIfinance.info, APPFINreport.info, FNWALLINform.info, developingcloud.info, smartfinancelist.com.

Q. Just three more, Mr. Brawner.

A. Scoreyourmoney.com, finshopland.me, and shopservice.live.

Q. What, if anything, did you do with these domains when you discovered evidence of them on Toppan Merrill's network?

A. We provided them to Toppan Merrill, as well as law enforcement.

Q. Are you familiar, based on your work in incident response, with the term "penetration testing"?

A. Yes.

Q. What is it?

A. Penetration testing is a discipline where security 09:53 professionals will attempt to break into a company in an authorized way, so a company will hire a security person or team to attempt to penetrate or break into their systems for purposes of identifying weaknesses or problems with their system.

Q. Had Toppan Merrill hired anyone to do penetration testing on its network in 2018, 2019, or 2020?

A. No.

Q. Let's talk about the Bridge system now, Mr. Brawner. Was that the second computer system at Toppan Merrill you were 09:54 describing?

A. Yes, it was.

Q. And what was Bridge again?

A. Bridge was an application used by its customers' publicly traded companies that need to prepare filings for the SEC. Bridge allows the preparer to sort of automate and speed and maintain accuracy of those filings in the preparation of those documents.

Q. Did Kroll find any accounts on the Bridge system for which it suspected unauthorized access?

A. Yes.

Q. And which accounts?

A. We identified approximately four accounts assigned to Toppan Merrill employees that were exhibiting suspicious behavior due to what they were being -- what they were doing.

09:55 Q. And what kind of access to the Bridge system did those employee accounts have, based on their usernames and passwords?

A. As employees, they had what we would call administrative access or broad access to the data within the Bridge application.

Q. And what would that mean in terms of being able to access the reporting of different companies?

A. So an account assigned to a Toppan employee would be able to view and see records from multiple other customers, as opposed to an account assigned to an individual customer who

09:55 would only be able to see their own documents.

Q. So if I worked for Coca-Cola company, what parts of the Bridge system would a Coke employee have access to?

A. I would only have access to Coca-Cola documents.

Q. But these employees that you described, how broad was their access?

A. It was broad. They could access documents for any companies that used the Bridge system.

Q. And did you review logs from the Bridge system in your investigation?

A. I did.

Q. What kind of activity did you see on these employees' accounts?

A. We saw these employees' accounts accessing and saving documents from multiple customers in short periods of time.

09:56 Q. What was done to those documents beyond access, if anything?

A. The logs show specific documents being opened and then saved to the local computer where the user at the time was.

Q. And what kind of documents?

A. These were draft and final documents for the SEC, so things like a 10K filing or a draft version of such.

Q. How far back did the logs that you looked at during your investigation go when you first started your investigation at Toppan Merrill?

09:57 A. Initially, the logs that we reviewed were available for approximately 90 days.

Q. Can I show you Exhibit 73, please. Do you have it in front of you, Mr. Brawner?

A. Yes.

Q. For starters, if Ms. Lewis can help us, can you tell us how many rows are in this spreadsheet?

(Witness examining document.)

A. 588.

Q. And what are these 588 rows?

A. Each row represents a log entry for the Bridge application.

Q. Any particular user?

A. As shown, the user is BenjaminOliver@ToppanMerrill.com.

Q. And do you see in Column A there's reference to dates and times?

09:58 A. Yes.

Q. What is the approximate date and time range for these 588 rows?

A. The earliest is October 14, 2019, and the latest is January 16, 2020.

MR. KOSTO: Ms. Lewis, if you'd kindly take us to the top, I'd like Mr. Brawner to describe for us what Column C is in this log.

A. Column C depicts the company name, the name of the customer of the Bridge system that the audit log pertains to.

09:59 Q. And I think you've touched on this, but Column D is what?

A. Is the username. This is the user that was logged into the application at the time of that event.

Q. And Column E, "Document Name"?

A. So document name, where there is a document related to the activity in the log, the name of the document in question is shown.

Q. So in Row 3, for example, what was the document acted on?

A. So in Row 3, a document named C_template_8K.

Q. And maybe just one more below it for a different example.

A. So on Row 12, it shows current_8K_earnings.

Q. And what client's area was that 8K earnings document from?

A. A client named Winmark Corp.

MR. KOSTO: Ms. Lewis, would you please take us to Column H.

10:00 Q. Is this column headed "Name"?

A. Yes.

Q. And what does it describe in the logs?

A. So each log entry, the application records the action that the entry relates to. So this provides insight into what the user was doing relative to each log entry.

Q. And what are the examples of things that appear in this first 30 or so rows?

A. So it starts with the entry "add-in start-up," which would depict the starting of the Bridge application for that user,
10:01 and then followed by things like "open folio at start-up," which would indicate a documentary filing that's being opened at the outset of using the application. And "add-in start-up" would be the launching of the Bridge application on the user's computer.

Q. How about "Save as Office" menu button there in Row 6?

A. If a user chose to save a copy of the document in question to their computer, for instance, using Microsoft Word, if you're familiar with clicking "save as" to save a copy of that document, that indicates the user chose that action.

Q. One last column to introduce us to. Could you look at Column G, please. What is "Machine Name"?

A. For each row in the log, the machine name is "USLEDGE," U.S. L-e-d-g-e.

Q. Was USLEDGE a machine name that you saw on employee
10:02 computers at Toppan Merrill during your review?

A. USLEDGE was not a Toppan Merrill computer.

Q. How do you know that? What's wrong with it?

A. By name, it does not match the convention that Toppan Merrill used.

Q. What was the convention?

A. So for a U.S. computer, as we discussed a bit earlier, it would be a U.S. with a D or L followed by a series of numbers.

MR. KOSTO: Ms. Lewis, if you could take us to Column A in the row "Date Time Stamp."

10:02 Q. Do you see references to the letter Z there, Mr. Brawner?

A. Yes.

Q. What does Z tell us about the dates and times in Column A?

A. So in a computer log, and in this log, the Z represents Zulu time, which is another name for UTC, or what we often think of as London time.

Q. And is that pretty standard in the forensics industry to have things go back to London time?

A. Yes.

Q. And Zulu is short for not having to say Coordinated Universal Time every time you want to talk about a time?

A. Correct.

Q. Okay. What are the times, in Zulu, for the first 35 or so rows, just, you know, the hour of day?

A. So it shows 9:00 a.m. and 10:00 a.m., Zulu time.

10:03 Q. And where were the computers and the computer users for the Bridge system?

A. In Central Time, typically.

Q. So what time did these actions take place in Central Time that are reflected in Exhibit 73?

A. So 9:00 a.m. would be 3:00 a.m. in U.S. Central Standard time, and, of course, 10:00 a.m. would be 4:00 a.m.

MR. KOSTO: One more line in Exhibit 73, Ms. Lewis, if you'd take us all the way to the bottom.

Q. What time did the actions reflected in this log take place, rows 587 and 588? 10:04

A. So these actions were on January 16, 2020, at 9:35 and 9:39 Zulu time.

Q. Can you convert that to U.S. Central Time for us?

A. So that would be 3:35 and 3:39 a.m.

Q. Moving from left to right, what company's records were accessed in these two log entries?

A. TPG Industries, Incorporated.

MR. KOSTO: And, Ms. Lewis, if you could take us over to the right edge. A little bit further, all the way.

Q. Do you see Column AA?

A. Yes.

Q. What are the numbers in rows 587 and 588 for Column AA?

A. They show the IP address of the user who was accessing Bridge and performing the listed actions.

10:05 Q. And can you read that IP address aloud, please, just one.

A. 185.228.19.147.

Q. At the time, what did you do with that IP address?

A. We provided that IP address to Toppan Merrill. We also researched that IP address to better understand where that IP address belonged, or what system on the Internet it might belong to.

Q. What system on the Internet did it belong to?

A. We found it associated with a company called AirVPN.

Q. What is AirVPN?

10:06 A. AirVPN is a company that provides customers with virtual network services. VPN stands for virtual private network, but most of us would typically use and purchase a VPN service to --

MR. NEMTSEV: Objection, your Honor.

THE COURT: Sustained, sustained.

Q. Do you have a simple example of what a VPN is to help the jury understand the term?

A. Many folks would use a VPN to change their location --

MR. NEMTSEV: Objection, your Honor.

THE COURT: So if you could just say, what is a typical use of a VPN?

THE WITNESS: Sure. It is to hide or change your actual location to be somewhere else in the interest of protecting your privacy --

MR. NEMTSEV: Objection, your Honor.

10:07 THE COURT: Overruled.

Q. Was AirVPN a provider you were familiar with at this time in your career?

A. No.

Q. Let me show you Government's Exhibit 74. Do you recognize it?

A. Yes.

Q. What is it?

A. It is additional Bridge application logs from January 21, 2020.

10:07 Q. And what user do these logs concern?

A. The username AJS1223@hotmail.com.

Q. Do you know who that user is?

A. Yes. It was Arthur Smallman.

Q. Did you mention his name before in your testimony?

A. Yes.

Q. In what context?

A. An earlier security event that we showed and you showed showing the Mimikatz activity on Arthur Smallman's Toppan Merrill computer.

Q. And what was Mimikatz?

A. It was a password dumping tool.

Q. About how many rows are there in Exhibit 74?

A. Thirty-one.

Q. What is the machine name from Column H associated with 10:08 each one of these rows?

A. The machine name was USLEDGE.

Q. And what is the IP address associated with each one of these rows?

A. The client IP address was 199.249.230.7.

Q. And just to be clear, when you say the client IP address, what IP address are we talking about?

A. So this would be the IP address of the computer associated with that connection to Bridge and that log-in by the Arthur Smallman account.

10:09 Q. Did you provide this address, this IP address to law enforcement?

A. Yes.

Q. What provider did this IP address come back to?

A. This IP address also came back to AirVPN.

Q. And what kinds of actions in Columns H did occur in these logs?

A. So the logs show the starting of Bridge, the opening of specific documents, and then the saving of those documents to the local user's computer.

Q. And in Column E, could you read the first couple kinds of documents that were accessed.

A. Row 3 shows IBM_EX99_1.

Q. What about row 10?

A. Row 10 shows AUB_earningsrelease_EX99_1.

10:10 MR. KOSTO: Ms. Lewis, could you take us to rows 26 to 28 of Exhibit 74.

Q. What company's records do these log entries concern?

A. Avnet, Incorporated.

Q. And in Column A, what time did the access to Avnet's records occur?

A. 14:28 Zulu, 14:29 --

Q. Can you flip that over to Central Time for us?

A. Sure. That would be approximately 8:28 a.m. U.S. Central Time on January 21.

10:11 Q. And what documents of Avnet's were accessed?

A. AVT_ex_99-1 or ex_99 dot -

MR. KOSTO: And, Ms. Lewis, all the way to the right. If Mr. Brawner could please read the IP address one more time.

A. 199.249.230.7.

Q. Did you find evidence on a Toppan Merrill system of the use of other IP addresses that started with 199.249.230?

A. Yes.

Q. And do you recall which?

A. I don't recall the last digit.

Q. Do you recall the provider that they were associated with?

A. They were each associated with AirVPN.

Q. And do you recall any that included the ending number .42?

A. Yes.

Q. What was that one used for.

10:12 A. .42 was seen in our logs, in the Toppan Merrill logs, accessing and attempting to access multiple web shells on the UIT application server.

Q. "Web shells" is a new term for us. Could you please define it.

THE COURT: Well, could you say the sentence again?

THE WITNESS: Sure. We saw connections being made to the UIT application server from the .42, the 199.249.230.42 IP address, attempting to access web shells on the UIT server.

Q. And that last question again was, what's a web shell?

10:12 A. So a web shell is code, or you can think of it as sort of a web page that's placed on a system by a threat actor, by a hacker, to provide back-door access into that system. So it's very small, hard-to-find pieces of code that permit someone to access a system --

MR. NEMTSEV: Objection, your Honor. Move to strike.

THE COURT: Overruled.

Q. One last exhibit, Mr. Brawner. Could we show you Government's Exhibit --

THE COURT: Can you say that in English again? I mean, I know it's English for you, but in plain speak.

Q. In even plainer English, what's a web shell?

A. So think of it as a secret way to get into a system without the knowledge of the system owner. So, for instance, if I sold padlocks that had the ability for me to set a 10:13 four-digit code to that lock, but when I manufactured it I always knew that, you know, 3456 would get me into that lock, but I didn't tell the owner of that lock that I could do that, in effect I'm creating a back door and a way to access whatever that lock is protecting.

THE COURT: So what's the web shell here?

THE WITNESS: So when you access a website, you're viewing information that is intended by the website owner, right? You're viewing documents or content. A hacker will, to get access to that underlying web server, will upload and place 10:14 code on that server, unbeknownst to the owner of that system, and they can use that to then connect in and manipulate the system.

THE COURT: It's a permanent access method?

THE WITNESS: Yes.

MR. NEMTSEV: And, your Honor, I would object to this line of testimony. He's not been noticed as an expert.

THE COURT: I can't hear a word you're saying.

MR. NEMTSEV: I said, I would object to this line of testimony. He's not been noticed as an expert, and yet he's testifying as an expert.

THE COURT: Overruled. Overruled.

Q. One last exhibit, Mr. Brawner. Exhibit 75, is this another kind of log?

A. Yes.

10:15 Q. Which system does it come from?

A. This is another log from the Bridge application.

Q. And with Ms. Lewis' help, could you help us figure out what time period the log covers?

A. So the first row is from January 21, 2020, and the last row is from January 16, 2019.

Q. So about a year, January, 2019, to January, 2020?

A. Yes.

Q. As we went by, did you see the machine name for each one of those rows?

10:16 A. Yes. Each row in Column D shows the machine named USLEDGE.

Q. Does this log show the company names and the type of documents like the others did?

A. No.

Q. Why, if at all, here did Kroll suspect problems with this log?

MR. NEMTSEV: Objection.

THE COURT: Sustained.

Q. Was USLEDGE an authorized computer on Toppan Merrill's system?

A. No.

Q. How did Kroll go about and how did you go about trying to secure the Bridge system after this incident response?

A. One of the steps that we advised Toppan Merrill to do was 10:16 to reset or change the passwords associated with the Bridge users where we saw the suspicious activity.

Q. And when did that occur, the password resets?

A. The Bridge password resets began in late January of 2020.

Q. And when was the last evidence that you found of unwelcomed guests on the Bridge system?

A. About the same time, so as the log shows, January 21, 2020.

MR. KOSTO: May I have one moment, your Honor? May I have one moment?

10:17 THE COURT: Oh, yes.

(Discussion off the record between government attorneys.)

Q. You testified about an IP address coming back to AirVPN, 185.228.19.147. Yes?

A. Yes.

Q. Did you provide that IP address to law enforcement?

A. Yes.

Q. What else did you provide to law enforcement in connection with your review?

A. Every IP address that our review found related to -- that we found as related to the intrusion, we provided to law enforcement.

MR. KOSTO: No further questions, your Honor.

MR. NEMTSEV: Your Honor, could we take a five-minute
10:18 break just to --

THE COURT: Excuse me?

MR. NEMTSEV: Could we just take a five-minute break?

THE COURT: No.

MR. NEMTSEV: No?

THE COURT: Unless it's a humanitarian need --

MR. NEMTSEV: I have a feeling this is going to take little longer than I initially anticipated, so I was hoping to use the bathroom before.

THE COURT: No. I mean, if you need to go, you need
10:18 to go. We'll just wait for you.

MR. NEMTSEV: No. I'll deal with it. Thank you, your Honor.

THE COURT: We usually take our breaks at 11:00, but if someone is --

A JUROR: I have a question.

THE COURT: No. Well, don't ask it. Write it down.

Maryellen, could you get the question.

THE CLERK: Just the piece of paper. Don't give me the notebook.

THE COURT: Well, why doesn't he get going, and then you can write it down and we'll pick it up, okay?

Oh, you have it. All right.

(Pause.)

THE COURT: The question is --

10:20 MR. FERNICH: Judge, before the question is asked, could we be heard on this briefly at sidebar?

THE COURT: Sure.

SIDEBAR CONFERENCE:

MR. FERNICH: It's not the subject matter of the question. It's the procedure of permitting the jurors to ask questions.

THE COURT: If they don't understand, I'll allow them to, but I'll allow you to see it first.

Do you want me to ask it or you to ask it?

10:21 MR. NEMTSEV: Your Honor to ask it.

THE COURT: I'm happy with the procedure. I was sort of screening. If it's a question that's sort of going to the burden of proof, I'm not going to allow it. If you just don't understand what a VPN is --

MR. FERNICH: It's a difficult procedure. I'm aware of an authority from the DC Circuit, the case was --

THE COURT: I understand, but let me just say this: This is highly technical. I'm having a hard time following it. Let me just start there. This is highly technical. I'm not getting realtime either, so I'm really struggling to get it. So if some juror doesn't understand a term, I'll allow it to be asked, but not if he's sort of trying to replace the burden of proof of the government. So I'm happy to have you ask it the way you want.

10:22 MR. KOSTO: What I propose, if you permit me to reopen the questioning and just ask this question in follow-up because this question will beg another question.

THE COURT: No.

(End of sidebar conference.)

THE COURT: Okay, the juror's question is -- and this is the way I'm going to do it. You know, I'm only going to let you ask about terms because it is, after all, the government's burden of proof here, so I can't let you sort of ask a ton of questions. So if you don't understand a term or what the term 10:23 means, as I said, just ask the question.

"Don't most computers use VPNs?"

MR. FRANK: I think it says "companies," your Honor.

MR. KOSTO: Yes, your Honor. It says companies, "Don't most companies use VPNs?"

THE COURT: Oh, you're right, "Don't most companies use VPNs?"

THE WITNESS: So as a term, VPNs are most often used for two purposes: One is to create a secure connection from your computer to your company. That's a common use case for a VPN. In the consumer market and in the commercial market, there are companies that provide VPN services. The technology is similar, but the use case for paying for your own VPN is often to provide a measure of anonymity or privacy for your connection. So if I'm sitting at home --

10:24 THE COURT: All right, that's probably enough.

THE WITNESS: Does that help?

THE COURT: Okay.

MR. KOSTO: The same objection as before which Mr. Nemtsev raised during the examination.

THE COURT: I don't know what you're referring to --

MR. NEMTSEV: The 702, your Honor.

THE COURT: What?

MR. NEMTSEV: The 702 expert issue.

Can I begin? Thank you.

10:24 CROSS-EXAMINATION BY MR. NEMTSEV:

Q. Mr. Brawner, we've never met before, correct?

A. Correct.

Q. We've never spoken either, correct?

A. No.

Q. You've spoken to the government agents in this case on multiple occasions; is that right?

A. Yes.

Q. Most recently, I believe January 11, 2023?

A. Yes, in preparation for being here today.

Q. And that was a meeting with the prosecutors in this case, potentially agents of the FBI, to go over the questions and answers that they're going to pose to you and the answers that you're going to give in this case; is that correct?

A. The only conversation with someone from the government in
10:25 that sense was with the attorney discussing the topics for my
testimony.

Q. You and I, we've never had a question-and-answer session before, correct?

A. No.

Q. And you've been with Kroll -- strike that. What is Kroll?

A. So Kroll is a global company that provides risk management and advisory services and cyber-security services to businesses and individuals.

Q. And as part of that offering of cyber-security services,
10:25 it offers penetration testing to its clients; is that correct?

THE COURT: I'm just having trouble hearing you.

Q. As part of its cyber-security offerings, Kroll offers penetration testing to its clients; is that correct?

A. Yes, we do.

Q. And how many other companies in the U.S. offer penetration testing?

A. I don't know.

Q. Would you say it's a common offering by cyber-security companies?

MR. KOSTO: Objection, foundation.

THE COURT: Overruled.

A. Yes. Many cyber-security companies offer penetration testing services.

THE COURT: How long were you with Kroll?

10:26 THE WITNESS: My work with Kroll dates back to 1999, and I've been in various roles at Kroll. There was a period that I was with a parent company to Kroll, but for most of my career, I've worked for Kroll.

Q. And Kroll in this case was first contacted after Toppan Merrill received an SEC subpoena; is that correct?

A. That's correct.

Q. And who, to your knowledge, brought Kroll into the investigation?

A. I don't recall.

10:27 Q. Was your contact first with Toppan Merrill, or attorneys for Toppan Merrill, or with the government?

A. I was not the engagement manager at the initiation of that contact, so I don't know for certain.

Q. Were you initially tasked with responding or helping Toppan Merrill respond to an SEC subpoena?

A. We were contacted at the point that Toppan Merrill had identified some suspicious activity on their network in response to an SEC subpoena.

Q. And from my recollection, your initial investigation only focused on one employee; is that correct?

A. No.

Q. Your investigation was not first focused on Mr. Oliver, Benjamin Oliver?

A. No.

10:27 Q. When did you identify Mr. Oliver as the potential employee that was compromised at Toppan Merrill?

A. So as part of the initial gathering of facts from Toppan Merrill, we learned that there were accounts on Bridge that were exhibiting unusual activity.

Q. And how many employees does Toppan Merrill have that have accounts with the Bridge program?

A. I don't know the exact number.

Q. Is it fair to say it's about 3,000?

A. It could be. I don't know.

10:28 Q. Do you recall if it has employees worldwide?

A. I know that Toppan has employees worldwide, yes.

Q. And those employees also have access to the Bridge program?

A. Some employees do. Not all employees.

Q. Did you ever meet Mr. Oliver?

A. No.

Q. Do you recall how many accounts Mr. Oliver had with Toppan Merrill that allowed him to access the Bridge system?

A. I recall one account in particular. I don't recall if he had more than one account. Some employees did have more than one account.

Q. Do you recall that Mr. Oliver in this case specifically had a Toppan Merrill email that had access to the Bridge account and a Hotmail email that had access to the Bridge 10:29 account?

A. I believe that is correct.

Q. And what is Hotmail?

THE COURT: What is --

MR. NEMTSEV: Hotmail.

A. Hotmail is an email service provided by Microsoft that's often used by consumers and individuals. It's a free email service.

Q. And is it your understanding that multiple Toppan Merrill employees used both the Toppan Merrill email address and their 10:30 Hotmail email address to access the Bridge environment?

A. In some cases, yes.

Q. Are you aware of Mr. Oliver using VPNs in connection with his position at Toppan Merrill?

A. I'm not aware of Mr. Oliver using any commercial VPNs, no.

Q. Do you know of any other users at Toppan Merrill that used commercial VPNs in connection with their positions?

A. No.

THE COURT: Did you go in and look?

THE WITNESS: That is not something that we specifically sought to validate across the whole company.

Q. And is my understanding correct that Mr. Oliver, and potentially other users, could add additional accounts into the Bridge system?

A. Yes. As an administrator, that access would be available.

10:30 Q. So they could potentially add a third account for themselves, or another account for somebody else, whether it's a client or one of the other approximate 3,000 employees that work for Toppan?

A. Yes. An administrator would have that ability.

Q. And based on your review of the Toppan Merrill system, am I correct that both drafts and final earnings reports were stored on that system?

A. That is my recollection, yes.

Q. And do you recall whether the FBI or the government in 10:31 this case asked Toppan Merrill, and potentially Kroll, to give you access to the actual documents that were potentially viewed?

A. No.

Q. Upon your examination of Mr. Oliver's account -- and I believe this was recorded in a memo, but if you recall it --

somebody said that he had poor password --

THE COURT: Could you start that again, please?

MR. NEMTSEV: Sure.

Q. In your conversations with the government, in your conversations with agents of the SEC and the FBI, I believe you mentioned that Mr. Oliver may have had poor password hygiene. Do you recall that?

MR. KOSTO: Objection.

THE COURT: Well, why don't you just ask the question
10:32 straight up.

You know, you're the one who did this investigation. Did he have poor passport hygiene -- password hygiene?

THE WITNESS: I don't recall specific to Mr. Oliver. When we see evidence of accounts that are compromised, that is a fair question when we're thinking about how that password might have been obtained improperly.

Q. And were there further conversations --

THE COURT: What does it mean, bad password hygiene?

THE WITNESS: So the idea of, let's say you have an
10:32 online bank account, and you protect -- your password for that account is "1234," right, or is an easy-to-know or easy-to-guess word or phrase, that would be indicative of poor hygiene because that password could be easily guessed or brute forced or compromised in some way.

Q. And was your concern that Mr. Oliver used the same password for Toppan Merrill as he used for his LinkedIn account?

A. I recall that question coming up at one point, yes.

Q. And that was a concern because LinkedIn, prior to that, was potentially hacked and data was potentially leaked from LinkedIn; is that correct?

A. That was one reason for the concern, yes.

THE COURT: Was his account at LinkedIn hacked?

THE WITNESS: I don't recall. At the time of that 10:33 question, we had not identified the source of the activity under Mr. Oliver's account.

Q. And there was also concern that Hotmail may have also been breached and may have also had its accounts compromised; is that correct?

A. Hotmail has had breaches in the past, and individual's accounts can be compromised, yes.

Q. And do you recall the type of device that was used to sign in to Mr. Oliver's account on the Bridge platform?

A. Mr. Oliver had a -- what we identified as the legitimate 10:34 or the authorized use of Mr. Oliver's account came from a Toppan Merrill computer.

Q. So what was necessary, to your knowledge, to access the Toppan Merrill Bridge system?

A. A username and a password.

Q. There was no other requirement?

A. There may have been additional requirements for some users. I don't recall today what those were.

Q. But for the bulk of users, including Mr. Oliver and Mr. Smallman, there was no requirement, for example, that they have two-factor authentication; is that correct?

A. No, not at that time.

Q. They weren't required to use a specific company laptop; is that correct?

A. No, because the customers could be from anywhere.

10:35 Q. And they could access the network from any IP address, whether it's a coffee shop, at home, or the office; is that correct?

A. Yes.

Q. And how would you rate Toppan Merrill's security --

MR. KOSTO: Objection.

Q. -- during the relevant time period?

THE COURT: Well, based -- overruled. Based on your experience since 1999.

A. We -- I did not review the overall security of Toppan 10:36 Merrill. We investigated two applications and related systems associated with the incident.

Q. But you testified that you made recommendations, certain recommendations to Toppan Merrill to change their security practices and to implement multifactor authentication; is that correct?

MR. KOSTO: Objection. Misstates the testimony.

THE COURT: Overruled.

A. So the Toppan Merrill Bridge application had measures of security. It had audit logging, as evidenced in my earlier testimony. The requirements for passwords and the requirements for users to log into that application, during the course of our investigation, we suggested that those requirements be strengthened. In that particular case, that is an application that's used by customers of Toppan Merrill. And so as a
10:37 business, the requirements are connected with the expectations of the customers, not necessarily your business as a whole.

Q. And Toppan Merrill, in particular, customers predictably would have high expectations of security, given that they're providing Toppan Merrill with draft earnings reports or other filings that they intend to be submitted to the SEC and kept confidential; is that correct?

A. I don't know the expectations of their individual customers, no.

Q. We went through several IP log files, and I was hoping to
10:37 explore with you Exhibit 73.

MR. NEMTSEV: Mr. Picard, could you please pull it up.

THE CLERK: Hold on. I have to switch over.

MR. NEMTSEV: Could we pull up Exhibit 73. That's 71. And can we go all the way to the left, Mr. Picard. Not the bottom, to the left. Perfect.

Q. So this is one of those log files that you testified about that shows a date, a username, a company name, a document name that was accessed, correct?

A. That is correct.

Q. In Columns AA, AB, AC, there is additional information concerning -- or additional information that you gathered.

MR. NEMTSEV: Could we go a little bit to the right, Mr. Picard.

Q. Column AA, for example, features the client IP address, 10:39 correct?

A. Yes.

Q. Column AB features the country of origin, correct?

A. Yes.

MR. NEMTSEV: Could we scroll down a little bit. A little further.

Q. And in some instances, the log files also feature a city and a country, correct?

MR. KOSTO: Objection, your Honor, foundation. This is the area --

10:39 THE COURT: This is your log, right? Did you prepare it?

THE WITNESS: This is the log from the Bridge system that we reviewed earlier, yes.

THE COURT: That your team prepared, right?

THE WITNESS: Yes.

THE COURT: All right, so I'll allow him to answer it.

MR. KOSTO: This is the subject we discussed before court this morning, your Honor.

THE COURT: Overruled.

Q. So in certain instances, there's also a city and a country and a potential county for the log-ins, correct?

A. Yes.

MR. NEMTSEV: Can we go a little further down, a little further.

10:40 Q. Here, for example, there's log-ins from Switzerland, log-ins from New York, correct?

A. Yes.

MR. KOSTO: The same objection, your Honor.

THE COURT: I'd like to know what they are. That means -- what do those locations denote? Do you know?

THE WITNESS: Yes. So this log is produced by the Microsoft cloud portion of the Bridge application. And prior to our investigation, the reason in Column AA there is not an IP address specified is, that tool was not configured to retain -- 10:40 it was essentially redacting the actual IP address from the log. However, it would capture the identified country or city of that IP address at the time of the connection.

THE COURT: Are you personally familiar with this?

THE WITNESS: I'm speaking from, yes, from my work on this particular investigation.

Q. Can we go a little further down. There's a connection from Minnesota, for example; is that correct?

A. Yes.

Q. Could we go a little further down. Another connection from New York? A little further. And ultimately connections from Kansas City, Missouri, correct?

A. Yes.

Q. You didn't find any connections from Boston, Massachusetts; is that correct?

10:42 MR. KOSTO: Objection.

THE COURT: Overruled.

A. I did not see any connections from Boston in this particular log, no.

Q. Or in any other log; is that correct?

MR. KOSTO: Objection.

THE COURT: Overruled.

A. I don't recall if there were connections from Boston in any other log.

Q. And there's also Column X, which indicates PC. Do you see that? 10:42

A. Yes.

Q. And is my understanding correct that this indicates that --

THE COURT: Excuse me. And so those locations were the IP address of what?

THE WITNESS: So that would be the IP address that was seen connecting to the application. So if you are, let's say, at home here in Boston and you connect to a server, that server may capture that IP address, and then one can correlate that IP address to a location based on other data to identify where in the world that IP address may be.

THE COURT: This is not something you yourself --

THE WITNESS: No.

THE COURT: All done off of a Microsoft application; 10:43 is that it?

THE WITNESS: In this case, the location data was provided automatically by Microsoft as part of the log being created.

MR. NEMTSEV: Maybe I can clarify, your Honor.

Q. Microsoft and the logging server system, once it senses a connection, it pulls data from that connection, correct? Like IP addresses, for example, what kind of username it is; in this instance, the location and the fact this connection occurred from a PC? Is that correct?

10:43 A. That's correct.

Q. And by PC, is my understanding correct that that's a Windows computer?

A. Typically a -- the word -- typically, PC would signify a Windows computer. I don't know in this log for certain if it's always a Windows computer. I believe it would be, though.

MR. NEMTSEV: Thank you, Mr. Picard. You can take this down.

Q. Did you also need a Crossfire application from the Toppan Merrill environment to view or access some of these earnings reports?

A. So part of the Bridge application was the website, the website that you would connect to. And then there was an additional component of the application that is installed on your computer, on the computer of the person accessing Bridge, 10:44 in this case, because the Bridge application is designed to work with Microsoft Office documents and spreadsheets, so there are what's called a plug-in or an additional application that interfaces with your Microsoft Word to work with Bridge.

Q. In simple terms, would you have to download that application in order to access a report from the Bridge environment?

A. Yes.

Q. Did you locate any information indicating who and when and how that application was downloaded by potential intruders?

10:45 THE COURT: By potential?

MR. NEMTSEV: Intruders.

THE COURT: Intruders.

THE WITNESS: I apologize. I would like to address my prior answer about the documents. So the plug-in is the typical interface to when a user is working with documents in

Bridge. I don't recall for certain if the plug-in is required in every instance of downloading a document; but when the plug-in is used, that provides us and provided the richest log detail about what the user was doing.

Q. So you don't know necessarily when and if that plug-in or that application, that Crossfire application, is required to view a certain report or not? Is that --

A. That is the typical workflow of a user that I saw. They would use the Crossfire application. I don't recall if it's 10:46 absolutely required in every instance.

Q. Did you observe how that application was downloaded or when by a potential intruder?

A. When a user logs on to the Bridge application, the website of Bridge, the ability to download that plug-in would be available through that application.

Q. Can we take a look at Exhibit 77A. And this is a spreadsheet of indicators of compromise, correct?

A. Yes.

Q. And you testified to some relevant ones, and you read that 10:47 list and indicated some of those IP addresses, but there's also portions that are redacted, correct?

A. Yes.

Q. And do those portions contain additional IP addresses, additional malware that was potentially located on Toppan Merrill servers?

A. The redacted portions, as best I recall, contained additional indicators of compromise.

Q. Additional indicators of compromise that may not have related to this specific instance of intrusion; is that correct?

A. In our investigation, all of the indicators we provided we believe were related to this intrusion.

THE COURT: That's a different question. What are the redacted? What's the redacted information? Were those other 10:48 intrusions?

THE WITNESS: No. They were all related to what we believed at the time to be this intrusion.

Q. Could we take a look at Exhibit 239, please.

MR. NEMTSEV: Sorry, your Honor, technical difficulties.

THE COURT: Is your mouse not working?

MR. FERNICH: It's just not loading.

MR. NEMTSEV: It's not clicking. Maybe we could ask Ms. Lewis to pull it up.

THE COURT: As you notice, the two key people in this 10:49 room are the paralegals, who know exactly where all of these documents are. Not that the attorneys aren't doing a great job, but these paralegals are essential. Here we go. Good.

Q. So this is one of the programs that was located on the Toppan Merrill servers; is that correct? If we could zoom in on the first half.

A. And so, yes. This is a log entry that we identified during our investigation.

Q. And in this particular instance, it's this program called "Mimikatz 2.0"?

A. Yes.

MR. NEMTSEV: And, Mr. Picard, could we go a little bit lower.

Q. And you can see here that it was created by a Joe Bialek, and you have his Twitter screen name?

10:50 A. That is the original author of the Mimikatz, this particular Mimikatz script.

Q. So this program, this software, it's wildly -- well, it's publicly available, correct?

A. Yes.

Q. Mr. Joe Bialek, he created it and he publishes it, and I can download it and you can download, and anyone in this room can download it at will?

A. Yes.

Q. And most of the programs that you've located on these

10:50 Toppan Merrill servers, they're publicly available? They're nothing special; is that correct?

A. No.

Q. Meaning I can't access some of these programs just by Googling them?

A. Most of the programs that we identified are publicly available. I can't confirm that all programs that we found were publicly available.

Q. But this one is, and I believe the first, DirBuster, as well?

A. That is publicly available, yes.

Q. Now, based on your investigation, did you determine who intruded into Toppan Merrill's servers?

A. No.

Q. Did you determine whether it's one person, a hundred
10:51 people, a thousand people?

A. No.

Q. Did you determine where they were located when these intrusions occurred?

A. No.

Q. So you have no idea who was on the other end of the keyboard, whether it's one person, a hundred, a thousand, or a million?

A. As a private citizen, as a commercial investigator, identifying where a person is and who is in a chair is
10:52 typically outside of the domain of a commercial company.

Q. And this is despite the fact that Kroll is considered one of the best companies in the industry?

A. That is correct.

MR. NEMTSEV: Nothing further, your Honor.

REDIRECT EXAMINATION BY MR. KOSTO:

Q. Mr. Brawner, Mr. Nemtsev asked you about DirBuster and Mimikatz. Do you remember that?

A. Yes.

Q. He suggests to you they were publicly available; is that right?

A. Yes.

Q. And there was nothing special about them?

A. Yes.

10:53 Q. What are those two programs used for?

MR. NEMTSEV: I object, your Honor. This goes back to, you know, what could he potentially use them for --

THE COURT: What?

MR. NEMTSEV: This goes to what could they potentially be used for.

THE COURT: Yes, sustained. He did an investigation, so --

MR. KOSTO: Mr. Nemtsev asked him --

THE COURT: What he observed them being used for in
10:53 this situation, I'll allow that.

Q. What did you observe those programs being used for in this incident response?

A. We saw DirBuster being used to guess valid files or pages on the UIT application. We saw Mimikatz being run to dump passwords from the memory of the computer; in this case, I believe Mr. Smallman's computer.

Q. Okay. Mr. Nemtsev asked you if you knew which of as many as a million people could have accessed Toppan Merrill's network; is that right?

A. Could you --

Q. Mr. Nemtsev asked you whether Kroll had determined which of as many as a million people had accessed Kroll's network; is that right?

A. I'm sorry. Could you repeat that one more time?

10:54 Q. Mr. Nemtsev asked you about the numbers of people who could have accessed Kroll's network, right?

A. Not Kroll's network but --

Q. I'm sorry. There's the confusion. Who could have accessed Toppan Merrill's network?

A. Yes.

Q. Did you determine characteristics of the individuals you suspected of unauthorized access?

MR. NEMTSEV: Objection.

THE COURT: Sustained.

10:55 Q. What did you notice in your review that was common across the logs that you reviewed?

A. We saw activity from a common computer name, and in that activity, a common pattern of accessing documents from multiple customers of Bridge, and saving those documents to the user's computer.

Q. And was that true for one IP address that you were looking into or more than one?

A. For more than one IP address.

Q. So how many different IP addresses of concern did Kroll identify during the investigation, just ballpark?

A. We identified approximately two dozen.

Q. And where did most of those IP addresses come back to for purposes of what provider they were associated with?

A. Most of them came back to AirVPN.

10:56 Q. And regardless of the IP address that it came from, did they show similar activity in terms of opening files, saving files, reviewing financial information off of Toppan Merrill's system?

A. Yes.

Q. And as the investigator there, what did that suggest to you about the number of attacker or attackers?

MR. NEMTSEV: Objection.

THE COURT: Sustained.

Q. Let me ask you a different question. There was some
10:56 testimony about Crossfire. Is that something -- is that something that comes along with the use of the Bridge application?

A. Yes.

Q. And did Kroll identify any logs of, you know, specific downloads of Crossfire on Toppan Merrill's network?

A. Crossfire was a component of the Bridge application, so it would -- its downloading could occur, you know, by any user of the application.

Q. And would the user of the application necessarily need to know that they were downloading it?

A. Yes.

Q. You testified about some location information --

THE COURT: So if you're hacking into Bridge, will you know that you've also downloaded through Crossfire?

10:57 THE WITNESS: Yes, the component, the Crossfire component, needs permission on your computer to integrate itself with your Microsoft Office application, so you would not be able to sort of install that without acknowledgement by the user in some way.

Q. In the case of the use of a VPN, would that go to the VPN computer or all the way back to the original user?

A. It would go back to the original user, whether or not they were traversing or using a VPN.

Q. You testified about some location information, and
10:58 Mr. Nemtsev showed you, I think, Minneapolis and New York and a few other places. Can you help the jury understand how that information arrives in the log. First of all, when it's turned on, is that in the Toppan Merrill log?

A. So those logs are created by the Microsoft platform, and at the time of the activity, there would have been an IP address captured. But the policy from Microsoft, the configuration of that application at the time did not permit the retaining of that IP address in the log, so oftentimes -- and sometimes that's done for, you know, for privacy or to protect information in some jurisdictions. So the log entries where there's 0000 would indicate that that had been redacted once that log was made available to Toppan Merrill.

THE COURT: It's a log of the IP address of the person who? Which person?

10:59 THE WITNESS: Whatever computer was accessing that application.

THE COURT: The intruders?

THE WITNESS: Could be, yes.

Q. And so if there are zeros there, was the logging turned on or off, in a simple way of thinking about it?

A. When there's zeros, there was no logging of the IP address.

Q. I'm asking specifically about the city/state pairs that Mr. Nemtsev asked you about. Where do the city/state pairs come when they do appear in the logs?

11:00 A. So they would have been --

Q. Is that something the Toppan Merrill system is, you know, adding in along with the --

A. No. That would have been added by the Microsoft platform automatically.

Q. And where was Microsoft obtaining the city/state information?

A. I don't know what source they use to make that correlation.

Q. Are there commercially available sources to obtain that information?

A. Yes.

Q. Are you familiar with any?

A. Yes.

Q. Such as?

A. There are commercial companies. One that comes to mind
11:00 would be MaxMind and other databases.

THE COURT: Do you know what was used here?

THE WITNESS: I don't know what Microsoft uses to make their correlation.

THE COURT: All right, stop. Stop there.

Q. Do you have any information about the accuracy of the information that the Microsoft software put into the Toppan Merrill logs?

A. No.

MR. KOSTO: If I could have a moment, your Honor.

11:01 (Discussion off the record between government attorneys.)

Q. Do you have any information about who traded in the documents associated with the access to Toppan Merrill's system?

A. No.

MR. KOSTO: No further questions, your Honor.

THE COURT: Anything?

MR. NEMTSEV: Maybe two minutes, three minutes?

THE COURT: Sure.

MR. NEMTSEV: Thank you.

THE COURT: Then we'll take our morning break. The snack is here, Maryellen has discovered.

RECROSS-EXAMINATION BY MR. NEMTSEV:

Q. Do you have any reason to dispute the accuracy of the 11:02 Microsoft logs --

MR. KOSTO: Objection.

THE COURT: Well, sustained as asked. Do you know one way or another, yourself personally?

THE WITNESS: To my experience is, those records are often accurate. They're not a hundred percent accurate. Sometimes they might represent a broad part of a region or country, but they don't -- they're not accurate down to a specific city, for example.

Q. Understood. And in your practice, in your experience as 11:02 an investigator for Kroll with 20 years of experience, you frequently rely on these sort of log files; is that correct?

MR. KOSTO: Objection, your Honor. Unrelated to his engagement here, which is the subject of his testimony.

THE COURT: Yes, sustained.

Q. You relied on these particular log files, and you believed them to be accurate; is that correct?

A. We did not rely on the location information in the logs.

Q. But the log files that were produced from Microsoft?

A. They were as produced from Microsoft.

Q. And you relied on them as they were produced from Microsoft, correct?

MR. KOSTO: Objection. Asked and answered.

THE COURT: Yes, sustained. Asked and answered.

MR. NEMTSEV: Could we take a look at Exhibit 77, but
11:03 only for the witness. I don't believe this has been admitted in evidence.

THE CLERK: 77A is in.

MR. NEMTSEV: Yes, could we take a look at 77 just for the witness?

THE CLERK: This doesn't work like that.

THE COURT: If you have it in writing, you can show it to him.

(Discussion off the record.)

MR. NEMTSEV: Nothing further, your Honor. I don't
11:03 want to default and break the system.

THE COURT: Hey, if there's one thing I have in here it's -- anyway, thank you very much. And you can leave now. Thank you.

(Witness excused.)

THE COURT: We can take our morning break. We'll start gathering around 11:25, and hopefully we'll be back out here at 11:30.

THE CLERK: All rise.

(Jury excused.)

THE COURT: Can I see counsel at sidebar for one second.

SIDEBAR CONFERENCE:

THE COURT: Who's your next witness?

MR. KOSTO: Our next witness is Mr. Oliver.

11:05 THE COURT: So what I didn't love was suddenly having an expert issue out of the blue. I gave opportunities for motions in limine. I'd show up at 8:30. So I allowed him in --

MR. KOSTO: We disclosed Mr. Brawner could talk about the incident response and terms that he would be using, and it wasn't objected to, so we didn't have the issue that we did with Mr. Clarke.

COURT: Well, he was the investigator. He has 25 years of experience. I allowed him in as 701, but it's great if I get a heads-up about this stuff. 11:05

MR. NEMTSEV: I didn't know what he was going to testify about.

THE COURT: "VPN" is the most common term.

MR. NEMTSEV: I didn't object to the VPN. The issue is when he starts to say, "This software can be used for this."

THE COURT: I sustained a bunch of those. Just give me a heads-up.

MR. NEMTSEV: The next expert from Stone Turn, Mr. Hartvigson, might be the same.

THE COURT: Okay, I'll be alert to it, but I only allowed him to testify to what he perceived in common terms in the computer world, but is there anyone who's an actual expert other than the statistician?

MR. NEMTSEV: Yes. I noticed Mr. Uitto.

11:06 MR. KOSTO: Mr. Uitto is the one who did the forensic exams of what the FBI seized in the investigation. He was not objected to. Mr. Kenny is another witness who was -- he was not objected to.

THE COURT: I need to be careful. Just this one took me by surprise. Anyway, I tried to rein it in, but I viewed him as more of a 701.

MR. FRANK: This is what they do.

THE COURT: At some point if it's this guy, what he perceived, because he went in and he really didn't have much to 11:07 say other than what he looked at, but there may be others that go far beyond that.

MR. NEMTSEV: Whatever the disclosure, they said he could summarize it. It wasn't like a true expert disclosure.

MR. KOSTO: But I think, given the context of the technical information, your Honor, the jury can get terms like

"IP address, domain."

THE COURT: Those are just basic terms.

MR. FERNICH: When he goes into what he observed outside his identification, what he typically sees in 25 years of experience, that's classic expert testimony.

THE COURT: Well, I sustained the objections when I realized where you were going.

MR. FRANK: And the defense was asking the same question.

11:07 MR. NEMTSEV: Well, we had to. We had to.

THE COURT: Anyway, so we'll get Oliver?

MR. FERNICH: Yes, our next witness.

THE COURT: Okay, we'll see you at -- we'll go right back out at 11:30, but give me a heads-up, okay? I'm a big heads-up person. All right, thank you.

(End of sidebar conference.)

(A recess was taken, 11:08 a.m.)

(Resumed, 11:38 a.m.)

THE CLERK: All rise.

11:37 (Court enters.)

THE CLERK: All rise for the jury.

(Jury enters.)

MR. KOSTO: The United States calls Benjamin Oliver, Your Honor.

THE CLERK: Sir, could you remain standing and raise your right hand.

BENJAMIN OLIVER, sworn

THE CLERK: Could you please state and spell your last name for the record.

THE WITNESS: My name is Benjamin Oliver. Last name, O-l-i-v-e-r.

THE CLERK: Thank you.

DIRECT EXAMINATION

BY MR. KOSTO:

11:39 Q. Keep your voice right up on that microphone. I'll do my best to keep my voice up as well, Mr. Oliver.

What city do you live in, sir?

A. Eden Prairie, Minnesota.

Q. Where do you work?

A. Toppan Merrill.

Q. How do you usually refer to Toppan Merrill, your employer?

A. Toppan Merrill.

Q. How long have you worked at Toppan Merrill?

A. I've worked there for four years, since the acquisition of 11:39 my previous company, Merrill Corp., which was -- I started at Merrill Corp. in 2011.

Q. So Merrill Corp. became Toppan Merrill?

A. Correct.

Q. Acquisition kind of situation?

A. Yes, sir.

Q. Okay. What's your educational background?

A. Bachelor's from UC Santa Barbara.

Q. What was your degree in?

A. Finance.

Q. What is Toppan Merrill?

A. Toppan Merrill's primarily a printing company, but they also do work in regulatory filings with the Securities and Exchange Commission.

Q. And who are Toppan Merrill's clients for regulatory filings with the Securities and Exchange Commission? 11:40

A. Pretty much any company that files publicly. It could be smaller companies to larger Fortune 500 companies. I also do work with some private equity deals.

Q. Does Toppan Merrill do specialized work only for small companies or only for the largest?

A. No, sir. It's across the board.

Q. What range of industries does Toppan Merrill's clients cover?

A. I'd call it pretty unlimited. It could be printing, banking, could be biotech. Across the board. 11:40

Q. Let me ask you about the names of some of the filings that Toppan Merrill helps its clients file. Okay?

Can we start with a Form 10-Q?

A. Yes, sir. That's a quarterly filing that a company that is publicly traded has to file with the SEC. It announces their performance over the last quarter.

Q. How many times per year?

A. Three times per year.

Q. And what kind of information goes into a quarterly report, a Form 10-Q?

A. The main item is their financial data, their performance for that given period of time.

Q. Can we contrast a 10-Q with a Form 10-K?

A. Yes, sir. So similar type of data, but a 10-K is an 11:41 annual filing. It's when a company is announcing their annual data for the previous fiscal year.

Q. And what type of data goes into the 10-K?

A. Similarly, the financial data for that given period.

Q. So far, 10-Q for quarterly, 10-K for annual?

A. Yes, sir.

Q. Total of four per year?

A. Correct.

Q. Can I add to that mix the 8-K?

A. Yeah. Outside of those periodic filings that a company 11:42 has to file, if a material fact were to come to play for that company, they also have a requirement to file that with the SEC. So typically something that has material relevance to their performance or something that's happening.

Q. In the real world, what kinds of things result in the filing of an 8-K with the SEC?

A. Very commonly, we'll see press releases. Companies will file their earnings releases. As an example, if a company were to change a CEO or something of that nature materially, they would have to report it.

Q. How about an acquisition or a sale of a company's division?

A. Absolutely.

Q. Big things in the life of the company?

A. Yes, sir.

11:42 Q. There's one other term I wanted to ask you about, which is an Exhibit 99. What is that?

A. Typically found within an 8-K. An 8-K really is kind of a shell of a document. It's three or four pages. The exhibit really contains the material facts of what the company is announcing.

Q. So what's the difference between the 8-K and the Exhibit 99?

A. The exhibit's really where the information is, the substance is, for what the filing is.

11:43 Q. And say there was a press release for whatever the company was announcing, would that be in the 8-K, or would that be in the exhibit?

A. That would be in the exhibit.

Q. And the exhibit, fair to say, is an attachment to the 8-K?

A. Yes, sir.

Q. What's your title at Toppan Merrill?

A. Senior director of client services.

Q. Did you have that role in 2019 and, let's say, 2020 up to about COVID?

A. My title -- the role would have been the same. My title would have been director. I was promoted since.

Q. And in that same time window -- I'll keep my questions to 2019 and early 2020 -- what did you do as a director of client services?

11:43 A. I was responsible for managing project managers. My project managing team were responsible for working directly with the client. My team would work with that client on their SEC filings, helping them getting from start to finish.

Q. You were a supervisor?

A. Yes, sir.

Q. Before Toppan Merrill files 10-Qs, 10-Ks, 8-Ks, Exhibit 99s with the SEC, how does Toppan Merrill treat that client information?

A. Very confidentially.

11:44 Q. Are there policies around confidentiality at Toppan Merrill?

A. Yes, sir.

Q. And what are they?

A. They range from having secure logins. We have training yearly on reminders of safety and security, confidentiality, and just some of the legal things related to it.

Q. Why, as a manager, do you have those policies?

A. To emphasize with our team regularly that it is -- our clients' data is the most important asset we have, really.

Q. And when Toppan Merrill is holding that information for its clients, is the public aware of that information?

A. No, sir.

Q. What is the name of the system that Toppan Merrill used to hold this confidential information?

11:45 A. The name's Toppan Merrill Bridge. Most people will call it Bridge for short.

Q. In your role as a manager in 2019 and 2020, did you access Bridge to handle your clients' filing needs?

A. Me personally, no.

Q. How is Bridge organized? First of all, how does one get access to it?

A. So to get access to Bridge, you have to have a login and password credentials.

Q. And if you were to go -- maybe paint a visual picture for 11:45 the jury -- you use your username, you use your password, you hit enter, what pops up?

A. As a person in my role, I would have access to all clients that we do business for, whereas a client would have access only to their personal information.

Q. So if you wanted to see -- I don't know if they're a client, but if you wanted to see IBM, what would you do?

A. I would log in using my credentials. There's a search bar. I would type in the entity's name and go to that entity's information.

Q. How often did you personally use Bridge to access client data before it was filed with the SEC?

A. Very infrequently.

Q. How often did you access Exhibit 99s, those 8-K-related documents, before it was filed?

11:46 A. Equally infrequently.

Q. What percentage of your job would you say was accessing client data in the Bridge system before it was filed?

A. Less than 2 percent.

Q. What were your work hours pre-COVID?

A. I typically was working in the office from 7:00 to 5:30 p.m. Central.

Q. When you say "in the office," where was that?

A. Saint Paul, Minnesota.

Q. And did you work off-hours in that time period?

11:47 A. I would work more in a consultative perspective. If some member of my team needed help, they would call me or email me. I have -- I manage three shifts around the clock, so I could get a call at any time.

Q. When you were supporting teammates in that way off-hours, were you at home?

A. Yes, sir.

Q. How often did you access the Bridge system from home to help a teammate?

A. I don't recall doing so.

Q. Before COVID, did you travel regularly for work?

A. Maybe once or twice that I can recall.

Q. When you were away from the St. Paul area, did you access the Bridge system in a consultative capacity?

A. Not that I recall.

11:48 Q. When you did access Bridge, how did you do so, what kind of machine?

A. I would use my personal laptop assigned by the company, and I would log in with my credentials.

Q. That's a piece of Toppan Merrill equipment that they own?

A. Yes, sir.

Q. Do you know the machine number that's associated with your laptop?

A. I would recognize it if I saw it.

Q. Do you know what letters it begins with?

11:48 A. NA.

Q. What is your username on the Toppan Merrill network?

A. It's gonna be first name, last name @toppanmerrill.com, so benjaminoliver@toppanmerrill.com.

Q. Do you use B Oliver or Ben O or anything like that?

A. It's different if I'm logging onto the network. Where I'm logging into the Bridge system, it's benjaminoliver@toppanmerrill.com.

Q. Do you recognize the machine name USLEDGE?

A. I do not, sir.

Q. Do you know what a virtual private network is?

A. I do.

Q. How would you explain it to the jury?

A. In our capacity, if we have to log onto our network, we would use a VPN system to, I guess, create a pipeline that 11:49 allows us onto our network to access network-related information.

Q. Is that something that the company, Toppan Merrill, gives to you, or do you have to go out and find your own virtual private network?

A. It's company provided.

Q. Are you familiar with virtual private networks that you can rent on your own, that the company doesn't give you?

MR. FERNICH: Objection.

THE COURT: Sustained.

11:49 Q. Do you use virtual private networks, other than the company's virtual private network, to log onto the Bridge system?

A. No, sir.

Q. Have you ever heard of AirVPN?

A. No, sir.

MR. FERNICH: Objection.

THE COURT: Overruled.

Q. Have you ever used AirVPN to log onto the Bridge network?

A. No, sir.

Q. I'd like to ask you a few questions about some specific employees at Toppan Merrill.

Do you know the name Arthur Smallman?

A. I do.

Q. Who is Mr. Smallman?

11:50 A. Arthur's a senior project manager who reports directly to me.

Q. How about May Vang?

A. She works as a doc specialist and reports directly to me.

Q. What's a doc specialist?

A. Doc specialists are a little different than a project manager. If a client asks for specific help within their document, the doc specialist would assist in that.

Q. What kind of help?

A. Formatting, something doesn't align right, they want it to 11:50 look different in HTML than the way it currently looks, if they're setting up a new table and would rather have our assistance than doing it themselves.

Q. Form rather than content; fair to say?

A. Absolutely.

Q. Who's George Zangara?

A. He's a senior project manager and reports indirectly to me.

Q. And Leah Anderson?

A. Is a project manager, reports to me.

Q. Were all these employees in 2019 and early 2020 employees with access to the Bridge system?

A. Yes, sir.

Q. Did these employees work off-hours?

How did they generally work? Let me ask that.

11:51 A. Sure. So all the names you mentioned work day shifts, meaning 7:00 to 3:30, or thereabouts, Central. We do have a weekly rotation whereby a project manager would then potentially work remotely over the weekend to cover our client needs.

Q. So Monday through Friday, if Mr. Smallman works 7:00 to 4:00, say, and there were a client issue, what happens at 5:00?

A. Our second shift, who comes on, say, 2:00 to 10:30 Central, would take care of that.

Q. And then at 2:00 in the morning, if there were an urgent

11:51 need for help from Toppan Merrill, would Mr. Smallman have to handle that during the week?

A. No, sir. We have a third shift.

Q. So it's really a 24/7 operation?

A. It's a 24-by-5 with weekend on call coverage.

Q. And other than when they're on weekend call, do your employees access the Bridge system from home?

A. No, sir.

Q. Do you know of a Rayna Behm?

A. I do.

Q. B-e-h-m?

A. Yes, sir.

Q. Who is Ms. Behm?

A. Rayna is a business analyst. She collects development requirements for our proprietary workflow system.

11:52 Q. I'm not sure what that meant, but I'll ask you whether she uses the Bridge system?

A. She does not.

Q. Do you know a Jerome Taylor?

A. I'm familiar with the name but not the individual.

Q. Is he a Toppan Merrill employee?

A. Yes, sir.

Q. Let me show you Government's Exhibit 73 in evidence. Directing you to Column D, do you see your username in Column D, like David?

11:52 A. Yes, sir.

Q. Could you read it aloud for the jury?

A. benjaminoliver@toppanmerrill.com.

Q. And Ms. Lewis will help with this, but can you -- with reference to the time stamp in Column A, can you give us the date range of entries in Exhibit 73, starting at the top?

A. 2019, October 14th.

Q. Going down to...

A. 2020, January 16th.

Q. Can I take you, with Ms. Lewis's help, back to the first seven rows.

Do you see reference to the company named Citi Group?

A. Yes, sir.

Q. Do you see reference in Column E to documents C_template_8-K, Exhibit 99.2, and EX_99?

11:53 THE COURT: You're going too fast.

MR. KOSTO: Let me slow down. Thank you, Your Honor.

Q. Do you see reference to C_template_8-K?

A. Yes, sir.

Q. Do you see reference, two rows down, to EX_99.2?

A. I do.

Q. Do you see reference to EX_99.3?

A. Yes, sir.

Q. Are all those in relation to Citi Group in Column C?

A. Yes, sir.

11:54 Q. Looking at that information, is that consistent with how you use the Bridge system in your job?

A. No, sir.

Q. Why do you say that?

A. Typically, I'm used in a consultative manner. A client or an employee typically will come to me and say, Ben, can you help me understand this item in this document? In which case, I may launch that document -- in this case, I'll just use the template 8-K as an example. I would look, I would guide them as to what I see and what to do.

What I see here is someone accessed the template 8-K --

MR. FERNICH: Objection.

THE COURT: Well, this is --

MR. KOSTO: This is your user account, Mr. Oliver, correct?

11:54 THE WITNESS: Yep. Uh-huh.

MR. FERNICH: He can't interpret the --

THE COURT: I'll allow whether or not you would use it this way.

THE WITNESS: Right. And I wouldn't. Typically, this --

MR. FERNICH: Objection.

THE COURT: What's the next question?

MR. KOSTO: Let me ask you to look at Column A for rows 2 through 8.

11:55 Do you see it there?

A. I do.

Q. What time is reflected on Column A for October 14th?

A. 9:13 a.m.

Q. Through what time?

A. 9:20 a.m.

Q. Do you see the reference to Z in the column?

A. Yes, sir.

Q. Do you know what that means?

A. I do not.

Q. You do not?

A. Do not.

Q. What time do you usually work for Toppan Merrill, not on weekends, and in the Bridge system?

A. 7:00 to 5:30 Central.

11:55 Q. Do you make a habit of working at 3:00 and 4:00 in the morning on the Bridge system?

A. I do not recall doing so.

MR. KOSTO: If you could take us to Column G, Ms. Lewis.

Q. Can I ask you to look at the machine name in Column G. She'll scroll from top to bottom. And I'll ask you if you recognize --

MR. KOSTO: Could you go back up there? Pause and then continue. And continue.

11:56 Q. In Column G, do you recognize any machine names?

A. Yeah, I'm really seeing two. One begins with an NA that, in looking at it, appears to be my computer. And one named USLEDGE.

Q. Do you recognize USLEDGE?

A. No, sir.

MR. KOSTO: If I could ask Ms. Lewis to sort on the NA500244 username for a second.

Q. Do you see that all these entries now concern that machine name, Mr. Oliver?

A. Yes, sir.

MR. KOSTO: And can I ask Ms. Lewis to bring us over to Column E.

Q. Do you see the documents referenced here?

A. I do.

11:57 Q. Is that consistent with how you used the Bridge system?

A. Yes, sir.

Q. Why do you say that?

A. In these instances, I'm opening one file in the whole filing submission. So an employee of mine would have asked me something specifically, and I would have gone specifically to that file.

Q. Would you, in using the Bridge system, open one file after another after another after another to get at something?

A. No, sir.

11:57 Q. Let me show you Government's Exhibit 75, please.

MR. KOSTO: If we could go to the top, Ms. Lewis.

Q. And I'll ask you if you recognize any usernames there?

A. I see my username.

MR. KOSTO: If Ms. Lewis could scroll a little bit.

Q. I'll ask you to tell us "stop" when you see another username.

A. Stop.

Q. Before I go on, did you ordinarily have that many interactions with the Bridge network in your work?

A. No, sir.

Q. What name appears below yours?

A. George Zangara.

Q. Is he an employee of yours?

A. Indirectly, he is.

11:58 Q. Does he use a USLEDGE machine?

A. No, sir.

Q. Do you and he both use the same laptop to access Toppan Merrill's Bridge system?

A. No, sir.

Q. Do you see Ms. Vang's name there, May Vang?

A. I do.

Q. Is she an employee of yours?

A. Yes, sir.

Q. Does she use a machine in USLEDGE to access Toppan Merrill's system? 11:58

A. No, sir.

Q. Do you and she share a computer to access Toppan Merrill's system?

A. No, sir.

MR. KOSTO: No further questions, Your Honor.

THE CLERK: Are you using the document camera at all?

MR. FERNICH: We may use 73, but that's it.

THE CLERK: All right. I'll switch it over just in case.

CROSS-EXAMINATION

BY MR. FERNICH:

Q. Good morning, Mr. Oliver. My name is Fernich and I'm a lawyer for Mr. Klyushin.

We don't know each other, do we, sir?

11:59 A. No, sir.

Q. We've never met or spoken?

A. No, sir.

Q. You last spoke with the government on January 6th?

A. No, sir.

Q. No? You didn't speak with the government on January 6th of this year?

A. That was not the last time I spoke with the government.

Q. Oh, you spoke with the government since January 6th?

A. Yes, sir.

12:00 Q. When was the last time you spoke with the government?

A. Last night.

Q. Last night.

And whom did you speak to from the government?

A. Seth.

Q. You spoke to one of the prosecutors in this case?

A. Yes, sir.

Q. Right. And he asked you some questions and you gave some answers?

A. Yes, sir.

Q. And that was all in preparation for your testimony here today, yes?

A. I would say, yes.

Q. Yes.

Now, you told us that you worked for Toppan Merrill or its 12:00 predecessor since 2011; is that correct?

A. Yes, sir.

Q. And that's about twelve years?

A. Yes, sir.

Q. And obviously, you're still working there now, right?

A. Correct.

Q. Okay. Now, turning back to the period 2019 through '20, you told us that Toppan Merrill handled sensitive financial information; fair to say?

A. Yes, sir.

12:00 Q. And you also told us that it was very important to keep that information confidential; am I right?

A. That's correct.

Q. And you worked at an office in Saint Paul, Minnesota; is that correct?

A. That's correct.

Q. You had the ability to work remotely, yes, the ability to do so?

A. The ability, yes.

Q. Yes. And the ability to work from home, if you wanted to or if you were told to, correct?

A. Correct.

Q. And you were using a Toppan Merrill laptop back at that time; is that right?

A. That's correct.

12:01 Q. And you would take the laptop home on weekends when you were on call?

A. In my role, I wasn't on call.

Q. You were not taking a laptop home on weekends before you became a director, for example?

A. The time you suggested, I'm the director.

Q. Yes. And you never took the laptop home on weekends, you weren't one of the people on call?

A. I was not on call, sir.

Q. Okay. But the employees who worked under you, they were on call, you told us, sometimes, correct? 12:01

A. That is correct.

Q. And they would take laptops home when they were on call, if you know?

A. I would say that's fair to say.

Q. Okay. And you could access Toppan Merrill's computer system through any WiFi connection; is that correct? If one were remote, a TM employee. It's a bad question. I'm sorry.

A. Can you rephrase that or restate it?

Q. Sure. A TM employee who was working remotely could access the computer system through any WiFi connection; is that correct?

A. That's correct.

Q. A Starbucks, for example?

A. That's correct.

12:02 Q. A McDonald's?

A. That's correct.

Q. Right. Okay. Fair enough.

And you could access Toppan Merrill's Bridge system, you told us, by entering a simple username and password pair; is that correct?

A. That's correct.

Q. You know what multifactor authentication is?

A. I do.

Q. There was no multifactor authentication system in place
12:02 back in 2019 through early '20 at TM, was there?

A. On the Bridge system, I don't recall.

Q. Right. And that's even though you told us that it was very important to maintain a secure environment? On direct, you told us that, right?

A. Can you restate the question?

Q. Yes. On direct, you told us that it was very important to have secure log-in credentials, correct?

A. That's correct.

Q. Because you were dealing with highly sensitive confidential information, correct?

A. Correct.

Q. Okay. And in fact, you know that Toppan Merrill didn't enable multifactor authentication for administrative users until late June of 2020; is that correct?

12:03 A. I wouldn't know the date or time.

Q. You don't disagree with me if I make that representation to you, do you?

MR. KOSTO: Objection.

Q. Sound about right, June 2020?

THE COURT: Just could you state the full question again?

MR. FERNICH: Sure.

Q. You don't disagree that TM didn't enable multifactor authentication until around late June of 2020?

12:03 MR. KOSTO: Objection. He stated he did not.

THE COURT: Overruled.

A. I don't know what the time frame was.

Q. Okay. But for sure, as you told us a moment ago, there was no multifactor authentication as early as, say, January 2020, right?

A. I don't believe there was.

Q. Okay. And, sir, like many of us, you had a LinkedIn account back around 2019 through '20?

A. Yes, sir.

Q. Did you use the same password for your LinkedIn account as any other email account you may have had?

A. I don't recall, sir.

Q. You don't recall. Fair enough.

Do you recall that LinkedIn suffered a widely reported
12:04 data breach just a few years ago? Are you aware of that?

MR. KOSTO: Objection.

THE COURT: Do you know one way or another?

THE WITNESS: I don't.

Q. Fair enough.

Back in 2019 through '20, Toppan Merrill had about 3,000 employees worldwide, yes?

A. I'm not sure, sir.

Q. Okay. Does that number sound correct to you?

A. I don't know, sir.

12:04 Q. Okay. Fair enough.

But you know that some 50 employees had administrator access to the computer system in your group alone; isn't that right?

A. I don't have 50 employees or ever have, so...

Q. In your group -- if somebody were to characterize your group, have you ever heard the phrase "your group" before?

A. I haven't, sir.

Q. Do you know what administrator access means?

A. I do.

Q. What does that mean?

A. An administrator access would have the ability to view all accounts under the Bridge system. It would also have the ability to create, delete user accounts or new accounts.

Q. Uh-huh. Did you have administrators with access 12:05 associated with your client services team?

A. Yes, sir.

Q. How many of those did you have, would you say?

A. Twenty.

Q. Twenty?

A. Approximately.

Q. Okay. Twenty with administrative access. Fair enough.

And you supervised roughly 12 employees on the client services team; is that right?

A. That sounds right during that time frame.

12:06 Q. Okay. And as you told us a moment ago, these -- I guess it was 20 administrators, they had broad access to any company using the Bridge system, data on any company using the Bridge system?

A. Can you define "broad access"?

Q. Strike "broad."

They had access to information on any company using the Bridge system, the administrators?

A. That's correct.

Q. Okay. And is it fair to say that some of your team members used more than one log-in credential, more than one log-in identity?

A. In the '19 to '20 time frame?

Q. Yeah.

A. That's correct.

12:06 Q. Okay. And team members could set up their other second log-in ID?

A. Administrators could, yes.

Q. Administrators could.

And what about a third log-in? Was it generally just two when we say more than one, or could they have three, four log-in IDs?

A. I'm only aware that anyone ever had two.

Q. Okay. And some TM employees, they also had Hotmail accounts associated with their Toppan Merrill Bridge accounts; 12:07 is that correct?

A. That's possible.

Q. Well, weren't you one of the employees who had a Hotmail address associated with your TM Bridge account?

A. I don't believe so, sir.

Q. Okay. What about -- well, it certainly wasn't unusual, was it, for a TM employee to have a Hotmail account associated with the Bridge account?

MR. KOSTO: Objection.

THE COURT: Do you know?

THE WITNESS: I wouldn't say it's unusual, but I wouldn't say it's usual.

Q. It wouldn't surprise you if that were true, correct?

A. No, I guess it wouldn't surprise me.

Q. Right. In fact, one of your own team members used a
12:07 Hotmail account for work purposes; isn't that correct?

A. I'm not sure, sir.

Q. Well, what about Arthur Smallman, did he have a Hotmail address that he used for work purposes?

A. I don't know, sir.

Q. You don't know.

MR. FERNICH: Tim, could we put up 73 in evidence. Let's stroll to the top. I'm sorry.

THE COURT: Are we going to take a stroll?

MR. FERNICH: I made a mistake.

12:08 Tim, try 75 in evidence instead.

But I wouldn't mind taking a stroll.

Q. Mr. Oliver, looking at Column C, lines 1 through 10, can you read the email address listed there? It appears to be an email address.

A. ajs1223@hotmail.com.

Q. That address, is that familiar to you?

A. No, sir.

Q. ajs, what was Arthur -- do you know if Arthur Smallman had a middle initial?

A. I don't, sir.

Q. Okay. Fair enough.

Sir, do you remember reading a few years back about a major data breach that Hotmail suffered?

A. No, sir.

12:09 MR. KOSTO: Objection. Relevance.

THE COURT: He answered "no."

Q. And, sir, besides Toppan Merrill employees, TM clients could also access the Bridge system; is that correct?

A. Yes, sir.

Q. About how many clients did TM have back in 2019 through '20, if you know?

A. I don't know, sir.

Q. More than a hundred?

A. Yes, that's fair.

12:09 Q. More than a thousand?

A. I can't say, sir.

Q. Definitely more than a hundred, though?

A. Yes, sir.

Q. Okay. Fair enough.

MR. FERNICH: Tim, can you put up 73 in evidence, please. Can you scroll down, please, Tim, to lines 55 through 57.

Q. Mr. Oliver, looking at 55 through 57 in Column A, can you tell us the dates of those entries, please?

A. 2019, October 16th.

MR. FERNICH: And, Tim, can you move it over to Columns AB, AC, and AD.

Q. Do you see those locations there in Columns AB, AC, and AD?

12:10 A. Yes, sir.

Q. Can you read those for the jury, please?

A. In AB is Prague. AC is -- I'm sorry. I'll mess this up.

Q. Yeah. And the country, if that's what it is, the next -- Praha. Do you know what Praha is?

A. Never heard of it, sir.

Q. Okay. Fair enough.

And the next word after Praha?

A. Czechia.

Q. Czechia. Okay, good enough.

12:11 And the government, they didn't show you AB, AC and AD or ask you about those columns on direct examination, did they? You don't remember that?

A. No, sir.

Q. Okay.

MR. FERNICH: Tim, can you scroll it over to the left a bit, the same columns. Keep going, keep going, keep going. All right. You can stop at D and E.

Q. Looking at lines 56 and 57, the final digits in 56 and 57, what are those? Can you read those?

A. What column, sir?

Q. I'm sorry. D and E, at the very end. Do you see where it says "X" there?

A. Oh.

Q. IBM slash --

12:11 A. EX99_1.

Q. Is that the 99 that you were talking about on direct, the Exhibit 99 that you were talking about on direct, do you know?

A. That would be common, yes.

Q. Yes.

And that Exhibit 99, typically, as you told us on direct, includes material facts like company announcements, yes?

A. It can, yes.

Q. It can.

And sometimes it includes press releases?

12:12 A. Correct.

Q. Okay. Good enough.

MR. FERNICH: Tim, 61 through 63, please.

Q. And the dates on those, sir, if you could give it to us?

MR. FERNICH: Tim, you have to move it all the way to the left. Very good.

Q. The dates on 61 through 63?

A. 2019, October 18th.

Q. Okay.

MR. FERNICH: And let's move it back to AB, AC, and AD, please.

Q. Can you read those locations in those columns, please?

A. In AB is Oslo. AC is Oslo County. AD is Norway.

Q. Okay.

MR. FERNICH: And let's scroll it back all the way to 12:12 the document column, the type of document column. There you go. 62 and 63.

Q. Those are also Exhibit 99s, it appears?

A. That's correct.

Q. Okay.

MR. FERNICH: And finally, let's take a look at 571 through 73, please. 571. You were there. Beautiful. Let's move it over to the left, past -- to A.

Q. Sir, if you don't mind, the dates on those?

A. 2019, December 4th.

12:13 Q. Okay.

MR. FERNICH: And, Tim, let's move it, again, AB, AC, and AD.

Q. Sir, can you tell us the locations that seem to appear in those columns? It's a hard one, the first one.

A. I was going to say, I'm going to blow it.

Q. I know.

A. Dietkon.

Q. Phonetic will be all right.

A. In AB. AC is Zurich. AD is Switzerland.

Q. Okay. Sir, can you take minute and look up and down --

MR. FERNICH: And, Tim, you can scroll it.

Q. -- and take as much time as you need, up and down Columns AB, AC, AD, and even AE. Go through it and take as much time as you want. I don't want to waste the jury's time.

12:14 MR. FERNICH: You can go a little faster than that or we'll be here all day.

Q. Sir, you don't see any reference to Russia anywhere in the entirety of that log in those columns, do you?

A. I did not, sir.

MR. FERNICH: Just a few more. We're almost done.

Q. Now, as part of your job as senior director of client services, the company would be working with the -- not directly with the SEC, but it was working to ensure that the documents met regulatory requirements; is that correct?

12:15 A. That is correct.

Q. And people at TM -- maybe not yourself -- they would provide some proofreading services of the documents, yes?

A. That is correct.

Q. For formatting?

A. Yes, sir.

Q. And also, again, to ensure regulatory compliance; is that correct?

A. Yes, sir.

Q. And in your experience, the Bridge system, it contained draft reports, yes?

A. Can you define "draft"?

Q. Well, let's ask it more directly.

The reports in the Bridge system could change before they were ultimately filed with the SEC?

12:16 A. Yes, sir.

Q. Okay. Fair enough. Thank you very much.

MR. FERNICH: No further questions.

REDIRECT EXAMINATION

BY MR. KOSTO:

Q. Good afternoon, again, Mr. Oliver. Mr. Fernich showed you a number of city and state and country pairs. Did you see that?

A. Yes, sir.

Q. In Exhibit 73; is that right?

12:16 A. Yes, sir.

Q. Do you have any idea about the accuracy of that information?

A. No, sir.

Q. Do you have any idea where it came from?

A. I do not.

Q. Do you have any idea whether it's a complete set of information?

A. I do not.

Q. Did you use a machine labeled "USLEDGE" to engage in edits or changes to documents on behalf of clients?

A. I did not.

Q. How do you know that?

A. The only system I've used to access Bridge was my computer, and it starts with an NA.

12:17 MR. KOSTO: No further questions, Your Honor.

MR. FERNICH: Just one or two. Do you want me to do it from here?

THE COURT: From right there is good.

RECROSS-EXAMINATION

BY MR. FERNICH:

Q. Sir, you don't know -- with reference to Exhibit 73, you don't know if the government or the defense introduced that exhibit into evidence, do you?

A. I do not.

12:17 MR. FERNICH: No further questions.

THE COURT: Thank you. You may step down.

Your next witness.

MR. KOSTO: The United States calls Daron Hartvigsen.

Can I give you some exhibit numbers?

THE CLERK: Yes.

MR. KOSTO: 71A, 71B, 71F, 71G, 71I, 71N, 71P, 71R.

THE CLERK: Thank you.

Sir, could you please stand and raise your right hand.

DARON HARTVIGSEN, sworn

THE COURT: I should ask -- I'm sorry. No objection?

MR. NEMTSEV: No objection, Your Honor.

THE COURT: All right. I'm sorry. Go ahead.

(Exhibit Nos. 71A, 71B, 71F, 71G, 71I, 71N, 71P, 71R received in evidence.)

12:19 THE CLERK: Could you please state and spell your last name for the record.

THE WITNESS: My last name is Hartvigsen, H-a-r-t-v-i-g-s-e-n.

MR. KOSTO: May I proceed, Your Honor?

THE COURT: You may.

DIRECT EXAMINATION

BY MR. KOSTO:

Q. Mr. Hartvigsen, go ahead and pull that microphone nice and close, and do your best to keep your voice up.

12:19 What city do you work in, sir?

A. Washington, D.C.

Q. And what field do you work in?

A. Cyber security.

Q. Are you familiar with the term "incident response"?

A. I am.

Q. What is incident response?

A. It's an organized approach to respond to a cyber incident or breach.

Q. How long have you worked in the incident response area?

A. About 25 years.

Q. Going from oldest to newest, what is your professional experience in the area?

A. Previously, I worked as a cybercrime investigator with the United States Air Force. And most recently, I've been
12:19 supervising and leading incident response teams.

Q. Go ahead and pull that microphone a little bit closer so we can hear you.

A. A little closer? Is that better?

Q. I think that's better.

A. Okay.

Q. Do you hold any professional certifications relevant to your work in incident response?

A. I do.

Q. What are they?

12:20 A. I'm a certified digital media collector, a certificated forensic examiner, and a certified cybercrime investigator.

Q. And what is a certified forensic examiner?

A. That's a person who can take digital evidence and examine it in a forensically sound way.

Q. Where do you work in December 2019 and January 2020?

A. I worked for a company named Ankura.

Q. At that time, had Ankura been hired on behalf of a company called Donnelley Financial Services -- or Donnelley Financial Solutions?

A. Yes.

Q. Solutions, not Services, right?

A. Correct. Solutions.

Q. What did you call it just in regular conversation?

A. We often called it DFIN.

12:21 Q. What was the problem at DFIN?

A. We were asked to look into an account that was suspected to be compromised.

Q. What was your role in the Ankura engagement for DFIN?

A. I lead the incident response teams.

Q. In a word or two, what was DFIN's business?

A. DFIN provided software solutions for public companies that needed to report their activities to regulators such as the SEC.

Q. And which of DFIN's computer networks was the first area 12:21 of concern for Ankura?

A. That was ActiveDisclosure.

Q. And what is ActiveDisclosure? How did that connect to DFIN's business?

A. ActiveDisclosure is essentially software that enabled DFIN clients or companies to collaborate and house documents and the like that would enable them to report information to the SEC, as an example.

Q. Where were the ActiveDisclosure computers located?

A. Chicago and in the cloud.

Q. What, if any, problems did Ankura identify with the ActiveDisclosure software program?

A. We identified activity -- unauthorized activity to a particular account.

Q. And how did the investigation suggest that that unauthorized access was occurring? 12:22

A. It was occurring from an IP address that was not normal for the account to come from.

Q. Which user account was involved at the first part of the investigation?

A. Julie Soma's account.

Q. Who was she?

A. She was an implementation architect for DFIN.

Q. Do you know what that is?

A. It's a person that helps build client environments in ActiveDisclosure. 12:23

Q. And as an implementation architect, what kind of permissions did she have on the system?

A. She had broad access. So access to all the client information.

Q. What location -- where does she physically work?

A. Out of Washington state.

Q. And where was Toppan Merrill's business headquartered -- excuse me, DFIN's business headquartered? I misspoke.

A. DFIN is located in Chicago, Illinois.

Q. Did Ankura look at Ms. Soma's company-issued computer?

A. We did.

Q. And were there any signs of unauthorized access on the physical computer itself?

A. Not on her computer, no.

12:23 THE COURT: By the way, I'm sort of -- what are you saying, Ankura? How do you spell that?

THE WITNESS: Ankura, A-n-k-u-r-a, that's the name of the company I worked for at the time.

THE COURT: That's the cyber security company?

THE WITNESS: Ankura does a number of client support across a broad spectrum of industries, but cyber security is one, yes.

Q. I won't ask you to name any competitors for context.

What was the problem with Ms. Soma's account, if there was 12:24 nothing on the computer itself?

A. The username and password was being used to access ActiveDisclosure in an unauthorized fashion.

Q. Did you and your team interview Ms. Soma?

A. We did talk to her, yes.

Q. And what did you talk to her about? General topics, not what you said.

A. Well, we were very interested in the times for which she normally would log into ActiveDisclosure, the normal area for which she would log in from, like her home ISP or whatnot. We were interested in understanding if some of the activity we saw on her account was something she recognized, those kinds of questions.

Q. And what did the information you learned from -- what did you do with the information that you learned from Ms. Soma about how she used her computer? 12:25

A. Well, we took what we learned and then looked at the log information and identified what we thought was legitimate activity and what we thought was suspicious activity.

Q. And how did you make that differentiation?

A. We looked at IP addresses, time of access, things like user-agent strings --

Q. Can I pause you there for a second?

A. Sure.

Q. We haven't heard that term before. What is a user-agent string? 12:25

A. A user-agent string is an artifact that is stored by computers or logs that -- some people attribute it to, like, a fingerprint of a browser that is used to access a system.

Q. So if I use Chrome, for example, would that generate one user-agent string?

A. Correct.

Q. And if I used Safari, would that have a slightly different user-agent string?

A. Exactly.

Q. How would that help in analyzing the usage on Ms. Soma's accounts?

A. So we knew what user-agent strings Ms. Soma normally had, and then user-agent strings that were different than that were suspicious.

12:26 Q. So you talked about user-agent strings. You talked about IP addresses and when she typically worked. Did you ask her questions about her use of virtual private networks?

A. Yes.

Q. And while we're on that subject, did DFIN offer its employees a virtual private network to connect to the ActiveDisclosure system?

A. DFIN had a corporate VPN that employees could use to access DFIN's systems.

Q. Can you distinguish that from a private virtual private network? 12:27

A. Yes. So a private virtual network is a connection between two computers or more that is intended to be private, that you can subscribe to or pay to. That's much different than the corporate DFIN VPNs.

Q. And was the access that was of concern to Ankura over the private VPNs or the DFIN corporate VPN?

A. It was the private VPNs.

Q. Did your investigation identify any other DFIN users whose accounts were suspected of being compromised?

A. Yes.

Q. Which?

A. Well, as a result of our work on Soma's account, we identified that there was an account associated with Ms. Han that also had suspicious access.

12:27 Q. Where did Ms. Han work physically?

A. Physically in Korea, South Korea.

Q. How about Mr. -- well, any others?

A. Yes.

Q. Whom?

A. Mr. Lewis, Jason Lewis.

Q. And where did he physically work?

A. Out of Texas.

Q. Do the names Emmaruth Gray and Asamnew Gebremarium and Noemi Oropez and Jennifer Heinzerling stick with you?

12:28 A. Yes, those accounts also had suspicious activity.

Q. And did you engage in the same kind of conversations and analysis with those employees that you did with Ms. Soma?

A. Yes.

Q. What kind of permissions did those other employees have, Han, Lewis, Gray?

A. Those users had broad access to client information on ActiveDisclosure.

Q. And why, if at all, did Ankura flag these accounts as potentially compromised?

A. Because they had similar IP address access, time of day, usage was not consistent with their normal course of business, and specifically VPN -- private VPN access.

Q. And where did Ankura find this evidence that it relied on?

A. On logs.

12:29 Q. And what kind of information did DFIN's logs track?

A. So --

Q. By way of example?

A. So DFIN's logs documented the time of connections, the user associated with that connection, the user account, the IP address that was a part of that connection, the user-agent string.

Q. How about the commands accomplished over the user's account?

A. Also documented commands, yes.

12:29 Q. And did the logs document what the user did while they were in the network?

A. Yes. What the user did on ActiveDisclosure, yes.

Q. So were ActiveDisclosure's logs -- can you just give us an idea of how big they were for the period you were looking at? What kind of volume are we talking here?

A. Very large. Millions of lines, gigabytes of information.

Q. And did Ankura -- how did Ankura go about narrowing that information down?

A. Well, we went with what we knew was good, and then what was suspicious. And so the connections that were suspicious, we investigated.

Q. Covering what time period would you say your -- what time period did your suspicions cover, as far as unauthorized access?

12:30 A. So we had logs back to the 5th of February 2018, and all the way up until 20 August 2020.

Q. And for Julie Soma's name in particular, how far forward did the logs go?

A. How far forward?

Q. From when to when? Julie Soma specifically.

A. From February of 2018 until January of 2020.

Q. Mr. Hartvigsen, I'm going to take you through just a few of those entries, okay?

A. Okay.

12:31 Q. Not all of the million.

MR. KOSTO: Can we please have Exhibit 71A.

Q. Do you see Exhibit 71A, Mr. Hartvigsen?

A. Yes, sir.

Q. Do you have your glasses fired up?

What is it?

A. This is an example of a message field in a log.
Q. Part of a log?
A. Yes.
Q. And for which ActiveDisclosure user was this message for?
A. This one is for rr52260, and that was Julie Soma.
Q. And where do you see rr52260?
A. On the fourth line down -- fifth line down.
Q. Is there a date and time associated with this message?
A. There is.
12:32 Q. What is it?
A. This is February 5th of 2018, and 7:16 and 50 seconds, what we call Zulu Time.
Q. Since you mentioned Zulu Time, what does that index to, where in the world is that?
A. London.
Q. If 7:16:50 is a London time, can you give us the approximate time on the West Coast of the United States?
A. So on the West Coast, Pacific Time, that would be the night of the 4th, so 11:16 on the 4th, in the evening.
12:32 Q. What, if anything, did that suggest to you when you were looking at this log in your investigation?
A. It was inconsistent with Julie Soma's normal behavior.
Q. What do the words "download.ASPX" on the second line of Exhibit 71A tell us?
A. It tells us that there was a download action.

Q. And what is a download?

A. A file was requested and downloaded.

Q. Does the message tell us what file?

A. It does.

Q. What is it?

A. Exhibit99_1.docx.

Q. And does the message tell us what DFIN client's document was accessed?

A. Yes. The source is Snap.

12:33 Q. The series of digits in the last highlighted row, do you see it there, starting with 209?

A. Yes. That's the IP address.

Q. What IP address are you talking about? The judge was about to ask --

A. Oh.

Q. -- what computer is that associated with?

A. So that would be the computer -- the IP address associated with the computer where that document would have gone.

Q. So the IP address where the document ended up?

12:33 A. Yes.

THE COURT: You mean the intruding computer?

THE WITNESS: Well, this would be the unauthorized --

THE COURT: The unauthorized computer.

THE WITNESS: -- computer.

THE COURT: Is that what you're saying that is?

THE WITNESS: Yes, ma'am.

Q. You're saying specifically that it's the IP address that obtained access to and downloaded a document from DFIN?

A. Correct.

Q. Okay. In the judge's words, "the unauthorized computer"?

A. That's right.

MR. KOSTO: Can we go to 71B, please. And we'll speed this up.

Q. But what date is this message from?

12:34 A. This is May 9th of 2018.

Q. What time?

A. 7:48 and 28 seconds.

Q. From which user's account?

A. It's Ms. Soma's.

Q. What was the action taken over the account?

A. This was a download.

Q. Of what company's document and what document?

A. What document? I'm sorry.

Q. What document and what client?

12:34 A. The source was HZNP, and the document was HZNP_master.docx.

Q. And can you tell the jury what IP address the document went to?

A. That's 119.204.194.11.

Q. And what time of day did this message occur, West Coast

United States?

A. That would have been the evening of the 8th, at 11:48 at night.

MR. KOSTO: Let's go to 71F, please.

Q. Just to move us along here, let me ask you, does this message come from DFIN's logs?

A. Yes.

Q. And is it for the user Julie Soma?

A. Yes.

12:35 Q. Does it reflect a download on October 22nd, 2018?

A. Yes.

Q. At approximately 1:21 in the afternoon?

A. Yes.

Q. Does that correspond to overnight hours on the West Coast of the United States?

A. It does. It would be about 5:00 in the morning.

Q. What was the company's information accessed here?

A. 99_1.docx.

Q. And could you read the IP address that the download went to? 12:36

A. 104.238.37.190.

MR. KOSTO: Could we please go to Exhibit 71G.

Q. Is this another message from Ms. Soma's user log?

A. It is.

Q. And is this a document that went to 104.238.37.197?

A. Yes.

Q. If you could combine these, what client and what document?

A. Tesla Motors. And so that would be 01updateletter.docx.

Q. Is there a 99 in front of that title?

A. Oh, I'm sorry, yes. I missed the 99, correct.

Q. Fair to say the date and time was October 24th, 2018, at 9:18 and 31 seconds?

A. That's correct.

Q. Without doing the exact math, is that overnight hours on 12:37 the West Coast of the United States?

A. Yes. That would be about 1:00 in the morning.

MR. KOSTO: Let's go to 71I, please.

Q. Another message from Ms. Soma's user log; is that right?

A. That's correct.

Q. What client's information?

A. KSS.

Q. And what document?

A. Exhibit99_1.docx.

Q. Overnight hours on May 20th, 2019, on the West Coast of 12:37 the United States?

A. Yes.

Q. What IP address was it sent to?

A. 209.197.20.204.

Q. Just a few more, Mr. Hartvigsen. I appreciate your patience.

A. Yes, sir.

MR. KOSTO: Could we see 71N.

Q. And I'll ask you if this is a message from Ms. Soma's user log?

A. It is.

Q. July 16th, 2019, at 6:38 in the morning, approximately?

A. Yes.

Q. Is that late in the evening, West Coast, United States?

A. It is.

12:38 Q. What's the client and what's the document?

A. The client source is Skechers, and the document is Q219_press_releaseSkechers.docx.

Q. What IP address did this download go to?

A. 209.197.20.198.

Q. Two more, Mr. Hartvigsen.

MR. KOSTO: Exhibit 71P.

Q. What client does this message concern?

A. KSS.

Q. What document?

12:38 A. Exhibit99_1.docx.

Q. To which IP address did it go?

A. 64.42.179.59.

Q. Is this a Ms. Soma user log?

A. It is.

Q. And what month and year are we in?

A. The month is November 15th, 2019.

Q. Can you convert 13:33:34 to West Coast, United States time?

A. Sure. That would be 5:33 and 34 seconds in the morning.

Q. Okay.

MR. KOSTO: 71R, please, Ms. Lewis.

Q. Can I have you read the username on this one?

A. Sure. It is rr146363.

Q. Is that a change from the last series of messages we've
12:39 been looking at?

A. It is.

Q. Whose user log is this?

A. This is a user log associated with Ms. Han.

Q. And where did Ms. Han work?

A. South Korea.

Q. What was the company and the document downloaded here?

A. Tesla Motors.

Q. And the name of the document?

A. TSLA-10-K_master.docx.

12:39 Q. And could you read the IP address that this document went to over Ms. Han's account?

A. 199.249.223.130.

Q. Do you recognize that IP address?

A. I do.

Q. Is it one that came up in the course of your investigation?

A. Yes.

Q. Who's the provider for that address?

A. AirVPN.

Q. And are you aware of how Ms. Han typically accessed DFIN's ActiveDisclosure network?

A. I am.

Q. Did she use private VPNs?

A. She used DFIN's VPN, normally.

12:40 Q. Once Ankura suspected unauthorized assess, for example, to Ms. Soma's account, did it take any steps, recommend anything to its client?

A. We did. As soon as we confirmed unauthorized access, we recommended that that account get suspended.

Q. And did DFIN follow Ankura's advice there?

A. Yes.

Q. Approximately when?

A. January of 2020.

Q. Did DFIN also recommend the suspension of Ms. Han's account when it discovered access like it saw? 12:40

A. Yes.

Q. When did that take place?

A. It was April of 2020.

Q. And Mr. Lewis, was that another name of an account where DFIN --

A. Yes. Jason Lewis's account, yes.

Q. And what recommendation did DFIN make for -- or did Ankura make for DFIN about that account?

A. We recommended that account also get suspended.

Q. Approximately what period -- and you may have said this -- did the logs that you reviewed show suspected unauthorized access to DFIN's network?

A. So February of 2018 until August of 2020.

Q. Did Ankura's investigation reveal any other networks on 12:41 DFIN's system that experienced unauthorized access?

A. Yes.

Q. And what system was that?

A. Active Directory.

Q. That has the same letters, AD, right?

A. Yes.

Q. ActiveDisclosure, if that's the software for the filing, what is Active Directory?

A. Active Directory is essentially a database of usernames and passwords used by a network to allow users access to 12:42 various resources on the network.

Q. What did you find on the Active Directory area where usernames and passwords were stored?

A. Unauthorized access.

Q. What specifically?

A. We found unauthorized entities acting as imposters or otherwise taking over accounts or making new accounts.

Q. By the way, are you familiar with the concept of penetration testing?

A. Yes.

Q. In a word or two, what is it?

A. It is a test of a network to identify whether or not you can penetrate it or access it.

Q. And in this 2018, 2019, 2020 time frame, had DFIN hired a firm like yours, or any others, to conduct penetration testing on its network? 12:42

A. No.

Q. Did Ankura find any unauthorized software on DFIN-issued computers?

A. We did.

Q. And what's another name for unauthorized software?

A. In this case, malware, malicious software.

Q. Where were the laptops that DFIN found -- or that Ankura found malware?

A. London and Poland.

12:43 Q. And what malware specifically was present on the London and Poland laptops?

A. They were renamed versions of a program called PowerShell.

Q. You said renamed?

A. Yes.

Q. What do you mean?

A. They were named something other than PowerShell to hide their presence.

Q. And now that we've said "PowerShell" a couple times, what does PowerShell mean to you?

A. Oh, PowerShell is a program that oftentimes administrators will use to conduct routine functions, like if a log source is filling up, before it fills up, that PowerShell can be programmed to do that move on a recurring basis without somebody at the keyboard.

12:44 Q. So you wouldn't need to be at the keyboard of the machine you were working on to access it?

THE COURT: So what does it do, PowerShell?

THE WITNESS: I'm sorry, ma'am?

THE COURT: In plain English, what does it do?

THE WITNESS: PowerShell is generally an administrator tool that is on -- can be put on systems that allow functions to be automated, so a person doesn't have to be at a keyboard for it to do its work. You can program it to do its work --

THE COURT: So an administrator takes over someone
12:44 else's computer?

THE WITNESS: It can take over administrative functions in a network without somebody being at that computer. So it can do things on somebody else's computer if you're -- if that makes sense.

THE COURT: So it's not malware?

Q. What's the difference, Mr. Hartvigsen, between a PowerShell program -- PowerShell.exe and renamed PowerShell?

A. So in this case, the renamed PowerShell was performing as malicious software because it was doing activities that were not functions that DFIN had programmed it to do.

Q. Did DFIN administrators run PowerShell under a different name?

A. DFIN administrators ran PowerShell under PowerShell. So if there was a legitimate reason for PowerShell to be used, it
12:45 would have been named PowerShell.

Q. So just one example, maybe, to illustrate this. You testified about logs, right?

A. Yes.

Q. Logs fill up?

A. Yes.

Q. Hundreds of thousands and thousands, right? At some point, does the computer run out of space?

A. That's correct.

Q. And can an administrator automate PowerShell to go in
12:45 every day or every other day or every other week, grab those logs and either delete them or move them to somewhere else?

A. Yes.

Q. And is that an example of something PowerShell can do in an automated fashion to administer the computer?

A. Yes.

Q. Okay. I'd like to ask you some questions about what PowerShell was doing on these laptops. Was it -- well, for starters, let's talk about the England laptop for a second.

A. Okay.

Q. So it had PowerShell on it?

A. It had a renamed version, yes.

Q. And what was the renamed version of PowerShell doing on the English laptop? What was it programmed to do automatically every time the machine booted up?

12:46 A. So when it started up, it attempted to delete the logs associated with its activity, and then it --

Q. Let me pause you there.

A. Oh, sure.

Q. Is deleting logs associated with PowerShell's activity, its own activity, something that DFIN would have PowerShell do?

A. No.

Q. What else did PowerShell do, this renamed PowerShell?

A. In this case, it attempted to collect usernames and passwords from that system.

12:46 Q. And what else did PowerShell do?

A. And then it connected to an external domain.

Q. Do you recall the name of the domain?

A. investmentcomp.com.

Q. And did you also look at a computer -- well, was connecting to investmentcomp.com part of DFIN's usual use for that computer?

A. No.

Q. And this is something PowerShell had it reaching out to every so often?

A. Yes.

Q. Now, you mentioned that there was PowerShell found on a computer in Poland as well; is that right?

A. That's correct.

Q. Was that regular PowerShell or renamed PowerShell?

12:47 A. It was a renamed PowerShell.

Q. And was renamed PowerShell something that DFIN administrators had put on this machine?

A. No.

Q. And what was PowerShell configured to do, this renamed PowerShell configured to do, on the Polish computer?

A. It was also set up to delete logs associated with its activity, collect usernames and passwords, and then connect to an external domain.

Q. What was that domain?

12:48 A. finauditsolutions.com.

Q. Did you say finauditsolutions.com?

A. Correct.

Q. And were these things part of the typical usage for that computer?

A. No.

Q. What was the earliest date associated with the PowerShell activity on the Polish laptop?

THE COURT: Well, can I just say, this Polish laptop, was that a DFIN laptop?

THE WITNESS: Yes.

Q. Was there a DFIN employee in Poland who was using it?

A. Yes, correct.

Q. Or worked in Poland and had this laptop from DFIN?

A. DFIN has a presence in Poland.

12:48 Q. But was it the Polish employee who was intentionally reaching out to finauditsolutions.com?

A. No.

Q. Was it the Polish employee who was deleting the logs?

A. No.

MR. KOSTO: If I could have one moment, Your Honor.

Thank you, Mr. Frank.

Q. What did you do with the domain names and the names of the Powershell renamed and the IP addresses associated with the activities on the Polish and English laptops?

12:49 A. We incorporated those into our investigative observations.

Q. And did you provide them to law enforcement, through the client or otherwise?

A. Can you repeat that?

Q. Did you provide the domains to the FBI?

A. I think DFIN's counsel did that, yes.

MR. KOSTO: No further questions, Your Honor.

Your Honor, may we approach briefly before Mr. Nemtsev --

THE COURT: How long do you think you have, Mr. Nemtsev?

MR. NEMTSEV: Twenty, 30 minutes. I don't think we'll make it by 1:00.

THE COURT: So why don't you go for ten minutes, and I'll deal with it at the break. Is it right now that you're going to be dealing with it? 12:50

MR. NEMTSEV: I don't think I'll make it to that portion.

THE COURT: Okay.

MR. KOSTO: Mr. Hartvigsen is in from out of town. If we can finish him, the government would ask that we do so.

(Interruption.)

THE COURT: We may need to have a break anyway. I'll see you at sidebar.

Why don't you stand and stretch.

12:51 **(SIDEBAR CONFERENCE AS FOLLOWS:**

THE COURT: Excuse me. We do not know why that juror just stepped out.

MR. KOSTO: Oh, dear.

THE CLERK: Judge, is it okay if one of the others steps out to use the restroom?

THE COURT: Yes. We are only going to be going another ten or fifteen minutes anyway.

THE CLERK: Go ahead.

THE COURT: What's the issue?

We're not going to finish.

MR. NEMTSEV: No.

MR. KOSTO: But we've just finished with Mr. Hartvigsen's exam. The government did not introduce any log information regarding geolocations for the reasons that we 12:52 discussed this morning. So there's no log information for Mr. Hartvigsen on geolocation.

I anticipate, having talked with Mr. Nemtsev, that he wants to show the cities and states and offer them for the purpose of showing that the access --

THE COURT: Whose document is it?

MR. KOSTO: Well, we haven't put the document in, and if they're offering it, we object to it based on --

THE COURT: This is his document?

MR. KOSTO: It's not his document. It's the company's 12:52 log, and we're objecting to so much of it as was generated by Microsoft, and we're not offering it because, as Mr. Nemtsev said in his motions, it's not reliable information.

THE COURT: I'll hear what he has to say. You're not using it?

MR. NEMTSEV: Oh, I need -- I need to use it. They need to use it, Your Honor. They just put in 71A through G. They're excluding 71. They put in evidence of maybe three or four, five unauthorized intrusions. If they want to prove an unauthorized intrusion, they need the log files.

MR. KOSTO: But they don't need the geolocation because it's not accurate.

THE COURT: I have to see what he has to say about. This whole thing is not about MaxMind, it's about Microsoft.

MR. KOSTO: It's the same thing.

12:53 THE COURT: Just as I said to them, please let me know in advance what the issue is.

MR. FRANK: We just found out today, Judge.

THE COURT: I'm going to let him ask a question and see what the guy says, but we're not going to finish today.

MR. NEMTSEV: No, but can we admit the log files?

THE COURT: No, I don't know if we can. I don't know if he knows anything about it.

MR. NEMTSEV: He just testified for an hour about log files that he reviewed.

12:53 THE COURT: Excuse me. I don't know if he knows anything about that information about geolocation.

MR. NEMTSEV: No. No.

THE COURT: Besides, it only covers part of it. Most of it isn't even mentioned. You're going to put in information about Boston, I assume.

MR. FRANK: We're putting in information about IP addresses, which is logs, but the location -- Microsoft's conclusion about where things come to, that geolocation data, that's precisely the same as the MaxMind data.

THE COURT: I don't know that. You have to get me something that says that. That's just you saying it.

MR. KOSTO: But they are the proponent of the general location here.

THE COURT: I've said what's sauce for the goose is
12:54 sauce for the gander. You have to live and die by that. So --

MR. KOSTO: When we proposed to offer this exact kind of information, the defense objected.

THE COURT: Listen, it was this crooked company called MaxMind.

MR. FRANK: No, Judge.

MR. KOSTO: Judge.

MR. FERNICH: That's not the crooked one.

THE COURT: That's not the crooked one? Which is the crooked?

12:54 MR. NEMTSEV: Micfo.

(Crosstalk.)

MR. FERNICH: MaxMind just makes it up. They're not crooked.

MR. KOSTO: Your Honor, this witness does not know --

THE CLERK: Are we okay?

THE CLERK: Yes, all good.

MR. NEMTSEV: Somebody is raising their hand.

QUESTION FROM JUROR (Is user agent string just different types of browsers?)

MR. NEMTSEV: I'm not sure what that question is asking.

THE COURT: I don't understand it either.

MR. KOSTO: I believe the question is asking whether the browser is the only thing that determines the user-agent 12:55 string. I believe the witness would say there are things other than the browser. So, for example, whether you're running Windows or Apple would also be something that comes--

THE COURT: You can do it on redirect if you want.

MR. NEMTSEV: I don't understand the question. I can't ask it.

(END OF SIDEBAR CONFERENCE.)

THE COURT: We won't finish this witness today, so we'll go another five minutes.

CROSS-EXAMINATION

12:56 BY MR. NEMTSEV:

Q. Good morning, Mr. Hartvigsen. Am I saying that correctly?

A. Hartvigsen, yes.

Q. My name is Max Nemtsev. I'm an attorney for Mr. Klyushin. Aside from a brief run-in in the elevator, you and I have never met today, correct?

A. We have not.

Q. We've never spoken, correct?

A. I'm sorry?

Q. You and I have never spoken; is that correct?

A. No, sir.

Q. You have spoken to the government, the FBI agents, and the prosecutors on several occasions; is that correct?

A. That is correct.

Q. And most recently was on January 6th, 2023, I believe; is that correct? 12:57

A. That sounds accurate.

Q. And at those meetings, one of the purposes for those meetings was to obtain information that you have, as well as to answer these agents' questions; is that correct?

A. They were to orient me to how this would all work.

Q. And they gave you the questions and solicited your responses for your testimony today; is that correct?

A. I think we went over logs and other things.

Q. And you've been part of the cyber security industry for 30 years; is that right? 12:57

A. Close to, yes.

Q. And right now, you're with a company called StoneTurn; is that correct?

A. I am.

Q. And before that, you were with a company called Ankura; is that correct?

A. Yes.

Q. And does StoneTurn offer approximately the same types of services as Ankura?

A. Yes.

Q. Do both of those services include penetration testing?

A. StoneTurn does not do penetration testing.

Q. But Ankura, another large cyber security vendor, they do; is that correct?

12:58 A. Correct.

Q. And are penetration testing offerings by cyber security companies common, to your knowledge, in the industry?

A. Yes.

Q. Am I correct that you were first contacted by DFIN following their receipt of a SEC subpoena?

A. We were contacted by DFIN's -- we were engaged by DFIN's lawyers as a result of that, I believe, yes.

Q. So DFIN's attorneys reached out to Ankura and reached out to yourself to hire you to help them analyze these very

12:58 enormous log files?

A. Exactly.

Q. Fair to say that you had a very large group of people working on this investigation from Ankura's side?

A. We had a number of specialties working on the case, yes.

Q. And how many people would you approximate worked on the investigation?

A. Twelve routinely.

Q. From different parts of the country? Any international ones, to your memory?

A. Yes.

Q. And DFIN, to your knowledge, is a company that services confidential information on behalf of publicly traded companies, amongst other businesses; is that correct?

A. Yes.

12:59 Q. And would you agree that excellent cyber security is a necessary component for companies like DFIN that hold such sensitive information?

A. I would agree that cyber security should be a consideration, sure.

THE COURT: I can't even hear you. A lot of times you're missing the mic. So please make --

THE WITNESS: Oh, I'm sorry.

THE COURT: Remember, you're speaking to them as well, so we all need to hear you.

01:00 THE WITNESS: Okay. Is that better?

THE COURT: Yeah.

Q. And DFIN had about 1,600 employees, to your knowledge?

A. I don't know.

Q. Do you recall how many accounts in total had access to DFIN's systems?

A. I don't recall.

Q. Greater than a hundred?

A. Yes, greater that a hundred, sure.

Q. Greater than a thousand, potentially?

A. I don't recall.

Q. Did you study the security features that were enabled for DFIN in 2018 to 2020?

A. We responded to unauthorized access; as a result, were exposed to some of those security features.

01:00 Q. Am I correct that the only thing that a user needed to do to gain access to DFIN's system is to enter a username and a password?

A. For ActiveDisclosure, yes.

Q. And ActiveDisclosure is primarily -- what you've reviewed, the log files that you reviewed came from that system; is that correct?

A. Yes.

Q. There was no two-factor authentication enabled; is that correct?

01:01 A. Not for ActiveDisclosure.

Q. There weren't access restrictions, meaning you couldn't access it from a public IP; is that correct?

A. I'm not sure I understand the question.

Q. Meaning you didn't have to be in DFIN's office to access the ActiveDisclosure system; is that correct?

A. No, you didn't have to be in DFIN's office.

Q. You could work from home, you could work from a cafe or you could work from a Starbucks; is that correct?

A. You could access it outside of DFIN's network, yes.

Q. And I believe you testified that your initial investigation was focused only on one employee by the name of Julia Soma?

A. That's correct.

Q. And as part of that investigation, did you obtain access 01:02 to all of Ms. Soma's devices?

A. We accessed her laptop that she used to conduct her business.

Q. Did you access her phone as well?

A. I don't recall.

THE COURT: You need to finish up this line of --

MR. NEMTSEV: Okay.

Q. And you reviewed her computer, and you found no malware installed on her devices; is that correct?

A. Correct.

01:02 MR. NEMTSEV: Judge, I could continue this tomorrow.

THE COURT: See you tomorrow morning, 9:00. Thank you.

THE CLERK: All rise.

(Jury exits.)

THE COURT: Thank you, sir. Could you stay on the stand just a couple more minutes?

Ask him about that geolocation information. I don't want to be doing this on the fly at sidebar.

MR. NEMTSEV: Can I ask him?

MR. KOSTO: May I inquire, Your Honor?

THE COURT: First, I want to show him the document and see if he knows anything about it.

MR. NEMTSEV: Could you please pull up that excerpt?

THE COURT: Please be seated.

01:04 Which document are we looking at?

MR. NEMTSEV: This is an excerpt from the one -- is it 70? I believe it's 70.

MR. KOSTO: 71.

MR. NEMTSEV: 71.

THE COURT: All right. Does that look familiar to you?

THE WITNESS: Yes.

THE COURT: So now, what do you want to ask him about?

BY MR. NEMTSEV:

01:04 Q. So this is just a small snippet of the millions of lines that were produced by the AD system; is that correct?

A. It appears so, yes.

Q. And this is what you relied on to determine whether Ms. Soma's account or somebody else's account may have been intruded upon; is that correct?

MR. KOSTO: Objection.

THE COURT: Overruled.

MR. KOSTO: This log is dozens and dozens of columns long, and he's asked him, This is what you relied on, and showed him five columns.

THE COURT: So you want the full breadth of all the columns?

MR. KOSTO: If he's going to ask him about this log, he should show him all the columns.

01:05 THE COURT: Yeah. Can you show him the whole spread of all the columns?

MR. NEMTSEV: Show him the next page.

It's just so lengthy, Judge, I split it by page from one to the other.

THE COURT: I know, but you're going to ask him about only one column, right?

MR. NEMTSEV: No, I'm going to ask him about several of them.

THE COURT: I'm not doing this as free-flowing
01:05 discovery. I'm just trying to get to the geolocation issue.

MR. NEMTSEV: Okay. Can we go down a little to the next page? No, next page.

BY MR. NEMTSEV:

Q. This column here. City name, continent code, continent code 2, country code, and the column a little bit further to the right.

THE COURT: Are you familiar with those columns?

THE WITNESS: I am.

THE COURT: You are? Okay. Did you generate that information?

THE WITNESS: I did not.

THE COURT: Where did you get it from?

THE WITNESS: These were already in the logs that we were provided.

01:05 THE COURT: So do you know anything about how that information was generated?

THE WITNESS: It's my understanding that they come from Microsoft when the logs are produced.

THE COURT: Based on all your years of experience and your certification, is this the kind of information Microsoft provides? Do you know?

THE WITNESS: So I don't know -- beyond what Microsoft puts in there, I don't know the source --

THE COURT: I can't hear you.

01:06 THE WITNESS: I'm sorry. Aside from the fact that they come from Microsoft, I don't know the source beyond that.

THE COURT: You don't know how they're generated?

THE WITNESS: No.

THE COURT: Do you know what it even is about?

THE WITNESS: Oh, sure. It's location information that is derived from the IP addresses that are in the logs.

THE COURT: But is that the IP address that's intruding? Are those the intruders?

THE WITNESS: It could be both, depending on --

THE COURT: What do you mean both? Both what?

THE WITNESS: Well, it could be the legitimate activity, so it would -- if there was legitimate activity from, like, Ms. Soma, it would show that, or it would show illegitimate --

01:07 THE COURT: It can either be the intruder or the one intruded upon?

THE WITNESS: Sure.

THE COURT: And there's no way of telling from here?

MR. NEMTSEV: No, Your Honor, this is only for the user --

THE COURT: I'm asking him. Can you tell what it is from here?

THE WITNESS: No, no. This is just a snippet of a Korea attribute.

01:07 THE COURT: Of a what?

THE WITNESS: South Korea's information.

THE COURT: He doesn't know what it denotes.

BY MR. NEMTSEV:

Q. You don't know that this is the IP location data for the IP that was used to access the server?

A. So we didn't use this information during our investigation. We didn't analyze this.

Q. You didn't analyze whether this IP came from, let's say, a location that Julia Soma does not work from? You've never used that?

A. We didn't use this for that information.

Q. Did you use a different system to determine that?

A. We did.

Q. What system did you use?

01:08 A. We used a tool called DomainTools, another tool called CentralOps that would --

Q. And did DomainTools provide results that are consistent with these logs?

A. We didn't do that analysis.

THE COURT: Okay. He doesn't know. If you have an expert, maybe your expert can put it in, but -- okay. But you can ask other questions. Thank you. I'll see you tomorrow morning.

THE WITNESS: Yes, ma'am.

01:08 THE COURT: How much longer do you have?

MR. NEMTSEV: Fifteen minutes, maybe less.

THE COURT: Fifteen.

How much on redirect?

MR. KOSTO: It depends on what happens tomorrow morning, but no more than that.

THE COURT: What?

MR. KOSTO: Depends on what happens, but no more than his --

THE COURT: I'm sorry you have to stay over. It's really going to be an utterly miserable day here with freezing cold, snow, and it's just horrible, but --

THE WITNESS: But you have good clam chowder, so I'm okay with it.

THE COURT: You're stuck here. It could be worse. It 01:09 could be Friday where it's going to be zero.

MR. KOSTO: Your Honor, I think we'll cover tomorrow -- assuming we finish up with Mr. Hartvigsen, we'll cover Mr. Garabo; Ms. Soma, whose use we've been talking about; Ms. Han, whose use we've been talking about; and Mr. Lewis, whose use we've been talking about. I think that will carry the day.

THE COURT: Assuming that the jurors get here on time.

I really do like to accommodate people from out of town. So if you let me know someone could be on a plane, just 01:09 let me know. That may be more pressure for you, but you can't say at ten of 1:00, Oh, he's from out of town. Okay? I can try and cut the break short or I can do other things to try and accommodate people.

MR. KOSTO: All of those witnesses are out of town, but I would expect, barring a late start, that we could do them all tomorrow.

THE COURT: Okay. Good. Thank you.

(Proceedings adjourned at 1:09 p.m.)

CERTIFICATE

UNITED STATES DISTRICT COURT)
DISTRICT OF MASSACHUSETTS) ss.
CITY OF BOSTON)

We, Lee A. Marzilli and Kathleen Silva, Official Federal Court Reporters, do hereby certify that the foregoing transcript, Pages 2-1 through 2-153 inclusive, was recorded by us stenographically at the time and place aforesaid in Criminal No. 21-10104-PBS, United States of America v. Vladislav Klyushin, and thereafter reduced by us to typewriting and is a true and accurate record of the proceedings.

Dated this 31st day of January, 2023.

/s/ Lee A. Marzilli
LEE A. MARZILLI, CRR
OFFICIAL COURT REPORTER

/s/ Kathleen Silva
KATHLEEN SILVA, RPR, CRR
OFFICIAL COURT REPORTER